PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-232776
(43)Date of publication of application : 27.08.1999

(51)Int.Cl. G11B 20/10
G09C 1/00
G11B 20/00
H04L 9/08
H04N 5/91
H04N 5/92
// H04N 7/167

(21)Application number : 10-027572
(22)Date of filing : 09.02.1998

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : YAMADA MASAZUMI
IIZUKA HIROYUKI
TAKECHI HIDEAKI
GOTO SHOICHI

(54) VIDEO RECORDING DEVICE AND REPRODUCING DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To make limitations of an effective reproduction period and the number of effective reproduction times of data sure by inputting the whole or a part of correspondence relation information of scrambled video and/or sound dataa ciphered scramble key and a ciphered key in which the scramble key is ciphered to a circuit and recording them on a video tape.
SOLUTION: A correspondence relation information generating means 11 generates data and hour information relating AV data which are scrambled with a recording scramble key Kss from a recording scrambling means 7 and a ciphered key Kc in which th recording scramble key Kss is ciphered. A MUX 12 inputs the key Kss from the recording scrambling means 7the ciphered key Kc from a ciphering means 10 and the data and hour information from the correspondence relation information generating means 11 to record them on a video tape 20. A reproduction descrambling means 17 inputs a key Kss from a key decoding means 16 and decrambles AV data with the key Kss to output descrambled data to a first DMUX 2. Thusth reproducing of the video tape is made possible only for a fixed period after it is recorded.

CLAIMS

[Claim(s)]

[Claim 1]A recording device comprising:

A scramble means which inputs a scramble key for carrying out the scramble of the data of said image and/or a soundand carries out the scramble of the data of said image and/or a sound with the scramble key while inputting data of an image and/or a sound.

An enciphering key generating means which generates an enciphering key for enciphering said scramble key.

A storing means which will eliminate the enciphering key if said enciphering key generating means stores an enciphering key by which it was generated and suits predetermined conditions of the enciphering key after that.

A key encoding means which inputs said enciphering key from said enciphering key generating meansand enciphers said scramble key with the enciphering key while inputting a scramble key from said scramble meansAn image by which scramble was carried out with said scramble keyand/or data of a soundA correspondence relevant information creating means which generates correspondence relevant information with an enciphering key which enciphered the scramble keyA recording device which inputs all or a part of an image by which scramble was carried out from said scramble means and/or data of a soundscramble key enciphered from said key encoding meansand correspondence relevant information from said correspondence relevant information creating meansand records them on a predetermined recording medium.

[Claim 2]The recording device according to claim 1 after said predetermined conditions is stored [said enciphering key]wherein it means exceeding predetermined time.

[Claim 3]Time into which said scramble means inputted data of said image and/or a sound as said correspondence relevant informationTime to which said scramble means carried out the scramble of the data of said image and/or a sound with said scramble keyTime at which said enciphering key generating means generated said enciphering keytime in which said storing means stored said enciphering keyThe recording device according to claim 1 or 2 being the information matched at time as which said key encoding means enciphered said scramble key with said enciphering keyor time at which said recording device recorded data of said image by which scramble was carried outand/or a sound on said predetermined recording medium.

[Claim 4]The recording device according to claim 1wherein said predetermined conditions mean that the number of times by which said enciphering key was used on the occasion of reproduction of data of said image and/or a sound by which scramble was carried out exceeds the predetermined number of times.

[Claim 5]The recording device according to any one of claims 1 to 4wherein it has a scramble key generating means which generates said scramble key and said scramble means inputs said scramble key from said scramble key generating

means.
[Claim 6]The recording device according to any one of claims 1 to 4wherein said scramble means inputs said scramble key from a broadcasting station and uses the scramble key.
[Claim 7]Playback equipment comprising:
Said correspondence relevant information according to any one of claims 1 to 6 from the predetermined recording medium according to any one of claims 1 to 6 is inputtedAn enciphering key acquisition means which specifies an image which it is going to reproduceand by which scramble was carried outand/or an enciphering key corresponding to data of a sound based on the correspondence relevant informationand searches and acquires said enciphering key in the storing means according to any one of claims 1 to 6.
While inputting an enciphered scramble key corresponding to data of said image which it is going to reproduce and by which scramble was carried out and/or a sound from said predetermined recording mediumA key encryption decoding means which inputs an enciphering key from said enciphering key acquisition meansand solves encryption of said said enciphered scramble key with the enciphering key.
While inputting data of an image by which scramble was carried out from said predetermined recording mediumand/or a soundA releasing scramble means by which a scramble key from said key encryption decoding means is inputtedand the scramble key cancels scramble of data of said image by which scramble was carried outand/or a sound.

[Claim 8]A recording device comprising:
A scramble means which inputs a scramble key for carrying out the scramble of the data of said image and/or a soundand carries out the scramble of the data of said image and/or a sound with the scramble key while inputting data of an image and/or a sound.
An enciphering key generating means which generates an enciphering key for enciphering said scramble key.
A storing means which stores an enciphering key which said enciphering key generating means generated.
A key encoding means which inputs said enciphering key from said enciphering key generating meansand enciphers said scramble key with the enciphering key while inputting a scramble key from said scramble meansAn image by which scramble was carried out with said scramble keyand/or data of a soundA correspondence relevant information creating means which generates correspondence relevant information with an enciphering key which enciphered the scramble keyA recording device which inputs all or a part of an image by which scramble was carried out from said scramble means and/or data of a soundscramble key enciphered from said key encoding meansand correspondence relevant information from said correspondence relevant information creating meansand records them on a predetermined recording medium.

[Claim 9]Time into which said scramble means inputted data of said image and/or a sound as said correspondence relevant informationTime to which said scramble means carried out the scramble of the data of said image and/or a sound with said scramble keyTime at which said enciphering key generating means generated said enciphering keytime in which said storing means stored said enciphering keyThe recording device according to claim 8 being the information matched at time as which said key encoding means enciphered said scramble key with said enciphering keyor time at which said recording device recorded data of said image by which scramble was carried outand/or a sound on said predetermined recording medium.
[Claim 10]The recording device according to claim 8 or 9wherein it has a scramble key generating means which generates said scramble key and said scramble means inputs said scramble key from said scramble key generating means.
[Claim 11]The recording device according to claim 8 or 9wherein said scramble means inputs said scramble key from a broadcasting station and uses the scramble key.
[Claim 12]Playback equipment comprising:
The correspondence relevant information according to any one of claims 8 to 11 from the predetermined recording medium according to any one of claims 8 to 11 is inputtedBased on the correspondence relevant informationan image which it is going to reproduce and by which scramble was carried outand/or an enciphering key corresponding to data of a sound are specifiedAn enciphering key acquisition means which it judges whether the enciphering key suits predetermined conditionstakes out the enciphering key from the storing means according to any one of claims 8 to 11 when agreeingand does not take out the enciphering key from said storing means when not agreeing.
While inputting an enciphered scramble key corresponding to data of said image which it is going to reproduce and by which scramble was carried out and/or a sound from said predetermined recording mediumA key encryption decoding means which inputs an enciphering key from said enciphering key acquisition meansand solves encryption of said said enciphered scramble key with the enciphering key.
While inputting data of an image by which scramble was carried out from said predetermined recording mediumand/or a soundA releasing scramble means by which a scramble key from said key encryption decoding means is inputtedand the scramble key cancels scramble of data of said image by which scramble was carried outand/or a sound.

[Claim 13]The playback equipment according to claim 12 after said predetermined conditions is stored [said enciphering key] in the storing means according to any one of claims 8 to 11wherein it means exceeding predetermined time.
[Claim 14]The playback equipment according to claim 12wherein said predetermined conditions mean that the number of times by which said enciphering key was used on the occasion of reproduction of data of said image and/or a sound by which scramble was carried out exceeds the predetermined number of times.

[Claim 15]A recording device comprising:
A scramble key generating means which generates a scramble key for carrying out the scramble of the data of an image and/or a sound.
A storing means which will eliminate the scramble key if said scramble key generating means stores a scramble key by which it was generated and suits predetermined conditions of the scramble key after that.
A scramble means which inputs a scramble key from said scramble key generating meansand carries out the scramble of the data of said image and/or a sound with the scramble key while inputting data of said image and/or a sound.
An image by which scramble was carried out with said scramble keyand/or data of a soundA correspondence relevant information creating means which generates correspondence relevant information with the scramble keyA recording device which inputs an image by which scramble was carried out from said scramble means and/or data of a soundand all or a part of correspondence relevant information from said correspondence relevant information creating meansand records them on a predetermined recording medium.

[Claim 16]The recording device according to claim 15 after said predetermined conditions is stored [said scramble key]wherein it means exceeding predetermined time.
[Claim 17]Time into which said scramble means inputted data of said image and/or a sound as said correspondence relevant informationTime to which said scramble means carried out the scramble of the data of said image and/or a sound with said scramble keyTime at which said scramble key generating means generated said scramble keytime in which said storing means stored said scramble keyOr the recording device according to claim 15 or 16wherein said recording device is the information matched at time which recorded data of said image by which scramble was carried outand/or a sound on said predetermined recording medium.
[Claim 18]The recording device according to claim 15wherein said predetermined conditions mean that the number of times by which said enciphering key was used on the occasion of reproduction of data of said image and/or a sound by which scramble was carried out exceeds the predetermined number of times.
[Claim 19]Playback equipment comprising:
The correspondence relevant information according to any one of claims 15 to 18 from the predetermined recording medium according to any one of claims 15 to 18 is inputtedA scramble key acquisition means which specifies an image which it is going to reproduceand by which scramble was carried outand/or a scramble key corresponding to data of a sound based on the correspondence relevant informationand searches and acquires said scramble key in the storing means according to any one of claims 15 to 18.
While inputting data of said image from said predetermined recording medium which it is going to reproduce and by which scramble was carried outsaid image corresponding to data of a sound by which scramble was carried outand/or a soundA releasing scramble means by which a scramble key from said scramble key

acquisition means is inputtedand the scramble key cancels scramble of data of said image by which scramble was carried outand/or a sound.

[Claim 20]A recording device comprising:
A scramble key generating means which generates a scramble key for carrying out the scramble of the data of an image and/or a sound.
A storing means which stores a scramble key which said scramble key generating means generated.
A scramble means which inputs a scramble key from said scramble key generating meansand carries out the scramble of the data of said image and/or a sound with the scramble key while inputting data of said image and/or a sound.
An image by which scramble was carried out with said scramble keyand/or data of a soundA correspondence relevant information creating means which generates correspondence relevant information with the scramble keyA recording device which inputs an image by which scramble was carried out from said scramble means and/or data of a soundand all or a part of correspondence relevant information from said correspondence relevant information creating meansand records them on a predetermined recording medium.

[Claim 21]Time into which said scramble means inputted data of said image and/or a sound as said correspondence relevant informationTime to which said scramble means carried out the scramble of the data of said image and/or a sound with said scramble keyTime at which said scramble key generating means generated said scramble keytime in which said storing means stored said scramble keyOr the recording device according to claim 20wherein said recording device is the information matched at time which recorded data of said image by which scramble was carried outand/or a sound on said predetermined recording medium.
[Claim 22]Playback equipment comprising:
The correspondence relevant information according to claim 20 or 21 from the predetermined recording medium according to claim 20 or 21 is inputtedBased on the correspondence relevant informationan image which it is going to reproduce and by which scramble was carried outand/or a scramble key corresponding to data of a sound are specifiedA scramble key acquisition means which it judges whether the scramble key suits predetermined conditionstakes out the scramble key from the storing means according to claim 20 or 21 when agreeingand does not take out the scramble key from said storing means when not agreeing.
While inputting data of said image from said predetermined recording medium which it is going to reproduce and by which scramble was carried outan image corresponding to data of a sound by which scramble was carried outand/or a soundA releasing scramble means by which a scramble key from said scramble key acquisition means is inputtedand the scramble key cancels scramble of data of said image by which scramble was carried outand/or a sound.

[Claim 23]The playback equipment according to claim 22 after said predetermined

conditions is stored [said scramble key] in the storing means according to claim 20 or 21wherein it means exceeding predetermined time.
[Claim 24]The playback equipment according to claim 22wherein said predetermined conditions mean that the number of times by which said scramble key was used on the occasion of reproduction of data of said image and/or a sound by which scramble was carried out exceeds the predetermined number of times.
[Claim 25]Said recording device data of an image by which scramble was carried out from said scramble meansand/or a soundEither of claims 1-6 having a charging means which imposes fee collection to record of said data when recording on said predetermined recording mediumOr either of claims 8-11either of claims 15-18or the recording device according to any one of claims 20 to 21.
[Claim 26]Either of claims 1-6wherein said predetermined recording medium is videotapeeither of claims 8-11either of claims 15-18or the recording device according to any one of claims 20 to 21.
[Claim 27]Either of claims 1-6wherein said predetermined recording medium is a hard diskeither of claims 8-11either of claims 15-18or the recording device according to any one of claims 20 to 21.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to the recording device which records the data of the image and/or sound to which the period about playback and the number of times were restricted by copyright etc.and the playback equipment which plays the data of the image and/or a sound.
[0002]
[Description of the Prior Art]NowAV information which has been the targets of copyright protectionsuch as a movie and musicis stored in videotape etc. The user can appreciate a moviemusicetc.when only a predetermined period when it says that such videotape etc. are one week through the rental store which lends out for pay borrows videotape etc. and plays it.
[0003]On the other handapart from the system of a rental of the videotape etc. which were mentioned above from progress of digital art and encoding technology etc. Programssuch as a movie from a broadcasting station and musicare inputted via a communications satellitethe scramble of the program is carried outit records on videotape etc.and the following are considered as recording playback equipment to play.
[0004]The block diagram of such conventional recording playback equipment is shown in drawing 7.
[0005]The receiving demodulation means 1 The picture image data of DEJIITARU of satellite broadcastingsound dataInputting EMM (individual information)ECM

(program information)and the enciphered broadcast scramble key Ks1st DMUX2 separates the picture image datathe sound dataEMMECMand the broadcast scramble key Ks from the receiving demodulation means 1. And the EMM decoding means 3 inputs the user ID key Kmdecodes EMM with the user ID key Kmand generates the work key Kw while it inputs EMM from the 1DMUX2. The ECM decoding means 4 inputs ECM and the enciphered broadcast scramble key Ks from the 1DMUX2decodes ECM with the work key Kwand restores the enciphered broadcast scramble key Ks while it inputs the work key Kw from the EMM decoding means 3.

[0006]Thenthe broadcast descrambling means 5 inputs the AV information by which scramble was carried out from the 1DMUX2is the broadcast scramble key Ks and descrambles the AV information by which scramble was carried out while it inputs the broadcast scramble key Ks from the ECM decoding means 4. And the broadcast descrambling means 5 is outputted to the record scramble means 7when outputting the descrambled AV information to 1st DMUX2 when displaying AV information on the display 21 directly in real timeand making AV information record on the videotape 20.

[0007]When the broadcast descrambling means 5 outputs AV information to 1st DMUX21st DMUX2 divides the AV information from the broadcast descrambling means 5 into picture image data and sound datait outputs picture image data to the video decoder 18and outputs sound data to the sound decoder 19. and the video decoder 18 and the sound decoder 19 -- each decodes the picture image data or sound data from the 1DMUX2and the display 21 displays an image and outputs a sound.

[0008]On the other handwhen the broadcast descrambling means 5 outputs AV information to the record scramble means 7the record scramble means 7While inputting the AV information from the broadcast descrambling means 5the record scramble key Kss from the 1st key generating means 6 is inputtedand the scramble of the AV information is carried out with the record scramble key Kss. AV information by which scramble was carried out with the record scramble key Kss is set to Kss (AV information).

[0009]With itgenerate the 2nd key generating means 8 and the enciphering key Kc for enciphering the record scramble key Kss the key encoding means 10While inputting the record scramble key Kss from the 1st key generating means 6the enciphering key Kc from the 2nd key generating means 8 is inputtedand the record scramble key Kss is enciphered with the enciphering key Kc. The record scramble key Kss enciphered by the enciphering key Kc is set to Kc (Kss).

[0010]And MUX12 inputs Kss (AV information) from the record scramble means 7and Kc (Kss) from the key encoding means 10and records them on the videotape 20.

[0011]When playing Kss (AV information) recorded on the videotape 20first2nd DMUX13 inputs Kss (AV information) from the videotape 20and Kc (Kss)and dissociates. And the key decoding means 16 inputs the enciphering key Kc from the 2nd key generating means 8decodes Kc (Kss) with the enciphering key Kcand

restores the record scramble key Kss while it inputs Kc (Kss) from the 2DMUX13. While the reproduction descrambling means 17 inputs Kss (AV information) from the 2DMUX13The record scramble key Kss from the key decoding means 16 is inputtedKss (AV information) is descrambled with the record scramble key Kssand the descrambled AV information is outputted to 1st DMUX2.
[0012]Finallythe AV information outputted to 1st DMUX2 is displayed as an image on the display 21 as well as the graphic display of the display 21 and the sound output in real timeand is outputted as a sound.
[0013]
[Problem(s) to be Solved by the Invention]By the wayalso in the future multi-channel digital-broadcasting agea user goes to a rental store each timethe point that videotape etc. must be borrowed etc. take time and effort as usual for a userand the system of a rental of the videotape etc. which were mentioned above is inconvenience.
[0014]Once it records [the conventional recording playback equipment mentioned above] AV information on the videotape 20if only it will use the enciphering key Kc from the 2nd key generating means 8the AV informationIt is reproduced any number of times and outputted as an image and/or a sound on the display 21 again always. Thusin conventional recording playback equipmentit will be said that there is no restriction between the effective regeneration phases of the AV information which has been the target of copyright protectionsuch as a movie and musicand in effective reproduction frequency. For exampleif recorded on a recording medium with the recording playback equipment which does not have restriction about a reproductive period or number of times which the AV information which has special value mentioned above like the movie immediately after theater televisingworth of the AV information will be reduced by half. That isthe broadcasting station cannot broadcast in comfort the AV information which has such special value.
[0015]This invention such conventional recording playback equipmentIf AV information is recorded on a recording mediumthe technical problem that neither during the effective regeneration phase of the AV information nor restriction of effective reproduction frequency is protected will be taken into considerationAV information is recorded on a recording medium and it aims at providing the recording device and playback equipment which observe during the effective regeneration phase of the AV informationand restriction of effective reproduction frequency.
[0016]
[Means for Solving the Problem]A recording device this invention of claim 1 is characterized by that comprises the following.
A scramble means which inputs a scramble key for carrying out the scramble of the data of said image and/or a soundand carries out the scramble of the data of said image and/or a sound with the scramble key while inputting data of an image and/or a sound.
An enciphering key generating means which generates an enciphering key for

enciphering said scramble key.
A storing means which will eliminate the enciphering key if said enciphering key generating means stores an enciphering key by which it was generated and suits predetermined conditions of the enciphering key after that.
A key encoding means which inputs said enciphering key from said enciphering key generating meansand enciphers said scramble key with the enciphering key while inputting a scramble key from said scramble meansAn image by which scramble was carried out with said scramble keyand/or data of a soundA correspondence relevant information creating means which generates correspondence relevant information with an enciphering key which enciphered the scramble keyA recording device which inputs all or a part of an image by which scramble was carried out from said scramble means and/or data of a soundscramble key enciphered from said key encoding meansand correspondence relevant information from said correspondence relevant information creating meansand records them on a predetermined recording medium.

[0017]Playback equipment this invention of claim 7 is characterized by that comprises the following.
Said correspondence relevant information according to any one of claims 1 to 6 from the predetermined recording medium according to any one of claims 1 to 6 is inputtedAn enciphering key acquisition means which specifies an image which it is going to reproduceand by which scramble was carried outand/or an enciphering key corresponding to data of a sound based on the correspondence relevant informationand searches and acquires said enciphering key in the storing means according to any one of claims 1 to 6.
While inputting an enciphered scramble key corresponding to data of said image which it is going to reproduce and by which scramble was carried out and/or a sound from said predetermined recording mediumA key encryption decoding means which inputs an enciphering key from said enciphering key acquisition meansand solves encryption of said said enciphered scramble key with the enciphering key.
While inputting data of an image by which scramble was carried out from said predetermined recording mediumand/or a soundA releasing scramble means by which a scramble key from said key encryption decoding means is inputtedand the scramble key cancels scramble of data of said image by which scramble was carried outand/or a sound.

[0018]A recording device this invention of claim 8 is characterized by that comprises the following.
A scramble means which inputs a scramble key for carrying out the scramble of the data of said image and/or a soundand carries out the scramble of the data of said image and/or a sound with the scramble key while inputting data of an image and/or a sound.
An enciphering key generating means which generates an enciphering key for enciphering said scramble key.

A storing means which stores an enciphering key which said enciphering key generating means generated.
A key encoding means which inputs said enciphering key from said enciphering key generating meansand enciphers said scramble key with the enciphering key while inputting a scramble key from said scramble meansAn image by which scramble was carried out with said scramble keyand/or data of a soundA correspondence relevant information creating means which generates correspondence relevant information with an enciphering key which enciphered the scramble keyA recording device which inputs all or a part of an image by which scramble was carried out from said scramble means and/or data of a soundscramble key enciphered from said key encoding meansand correspondence relevant information from said correspondence relevant information creating meansand records them on a predetermined recording medium.

[0019]Playback equipment this invention of claim 12 is characterized by that comprises the following.
The correspondence relevant information according to any one of claims 8 to 11 from the predetermined recording medium according to any one of claims 8 to 11 is inputtedBased on the correspondence relevant informationan image which it is going to reproduce and by which scramble was carried outand/or an enciphering key corresponding to data of a sound are specifiedAn enciphering key acquisition means which it judges whether the enciphering key suits predetermined conditionstakes out the enciphering key from the storing means according to any one of claims 8 to 11 when agreeingand does not take out the enciphering key from said storing means when not agreeing.
While inputting an enciphered scramble key corresponding to data of said image which it is going to reproduce and by which scramble was carried out and/or a sound from said predetermined recording mediumA key encryption decoding means which inputs an enciphering key from said enciphering key acquisition meansand solves encryption of said said enciphered scramble key with the enciphering key.
While inputting data of an image by which scramble was carried out from said predetermined recording mediumand/or a soundA releasing scramble means by which a scramble key from said key encryption decoding means is inputtedand the scramble key cancels scramble of data of said image by which scramble was carried outand/or a sound.

[0020]A recording device this invention of claim 15 is characterized by that comprises the following.
A scramble key generating means which generates a scramble key for carrying out the scramble of the data of an image and/or a sound.
A storing means which will eliminate the scramble key if said scramble key generating means stores a scramble key by which it was generated and suits predetermined conditions of the scramble key after that.
A scramble means which inputs a scramble key from said scramble key generating

meansand carries out the scramble of the data of said image and/or a sound with the scramble key while inputting data of said image and/or a sound.
An image by which scramble was carried out with said scramble keyand/or data of a soundA correspondence relevant information creating means which generates correspondence relevant information with the scramble keyA recording device which inputs an image by which scramble was carried out from said scramble means and/or data of a soundand all or a part of correspondence relevant information from said correspondence relevant information creating meansand records them on a predetermined recording medium.

[0021]Playback equipment this invention of claim 19 is characterized by that comprises the following.
The correspondence relevant information according to any one of claims 15 to 18 from the predetermined recording medium according to any one of claims 15 to 18 is inputtedA scramble key acquisition means which specifies an image which it is going to reproduceand by which scramble was carried outand/or a scramble key corresponding to data of a sound based on the correspondence relevant informationand searches and acquires said scramble key in the storing means according to any one of claims 15 to 18.
While inputting data of said image from said predetermined recording medium which it is going to reproduce and by which scramble was carried outsaid image corresponding to data of a sound by which scramble was carried outand/or a soundA releasing scramble means by which a scramble key from said scramble key acquisition means is inputtedand the scramble key cancels scramble of data of said image by which scramble was carried outand/or a sound.

[0022]A recording device this invention of claim 20 is characterized by that comprises the following.
A scramble key generating means which generates a scramble key for carrying out the scramble of the data of an image and/or a sound.
A storing means which stores a scramble key which said scramble key generating means generated.
A scramble means which inputs a scramble key from said scramble key generating meansand carries out the scramble of the data of said image and/or a sound with the scramble key while inputting data of said image and/or a sound.
An image by which scramble was carried out with said scramble keyand/or data of a soundA correspondence relevant information creating means which generates correspondence relevant information with the scramble keyA recording device which inputs an image by which scramble was carried out from said scramble means and/or data of a soundand all or a part of correspondence relevant information from said correspondence relevant information creating meansand records them on a predetermined recording medium.

[0023]Playback equipment this invention of claim 22 is characterized by that

comprises the following.
The correspondence relevant information according to claim 20 or 21 from the predetermined recording medium according to claim 20 or 21 is inputtedBased on the correspondence relevant informationan image which it is going to reproduce and by which scramble was carried outand/or a scramble key corresponding to data of a sound are specifiedA scramble key acquisition means which it judges whether the scramble key suits predetermined conditionstakes out the scramble key from the storing means according to claim 20 or 21 when agreeingand does not take out the scramble key from said storing means when not agreeing.
While inputting data of said image from said predetermined recording medium which it is going to reproduce and by which scramble was carried outan image corresponding to data of a sound by which scramble was carried outand/or a soundA releasing scramble means by which a scramble key from said scramble key acquisition means is inputtedand the scramble key cancels scramble of data of said image by which scramble was carried outand/or a sound.

[0024]
[Embodiment of the Invention]Belowan embodiment of the invention is described with reference to drawings.
[0025](Embodiment 1) The composition of the recording device of the embodiment of the invention 1 and playback equipment is described first.
[0026]The block diagram of the recording device of the embodiment of the invention 1 and playback equipment is shown in drawing 1. The recording device of ******** comprises:
The 1st key generating means 6.
Record scramble means 7.
The 2nd key generating means 8.
KcFIFO9the key encoding means 10the correspondence relevant information creating means 11and MUX12.
The playback equipment of ******** comprises:
The 2DMUX13.
Enciphering key acquisition means 14.
Kc latch means 15.
The key decoding means 16 and the reproduction descrambling means 17.
The receiving demodulation means 11st DMUX2the EMM decoding means 3the ECM decoding means 4the broadcast descrambling means 5the video decoder 18and the sound decoder 19 are also displayed on drawing 1. The videotape 20 as a recording medium and an image are displayedand the display 21 which outputs a sound is also displayed.
[0027]The receiving demodulation means 1 is a means to input the picture image datathe sound dataEMM (individual information)ECM (program information)and the enciphered broadcast scramble key Ks of DEJIITARU from a broadcasting station via a communications satelliteand to operate those all or some signal wave forms orthopedically.

[0028]The picture image data and sound data which the receiving demodulation means 1 inputs are the data by which scramble was carried out with the broadcast scramble key Ks. Belowwhen you mean both picture image data and sound datalet picture image data and sound data be AV information.
[0029]EMM (individual information) which the receiving demodulation means 1 inputs is information which is needed when generating a key called the work key Kw explained later.
[0030]ECM (program information) which the receiving demodulation means 1 inputs is information which is needed when restoring the enciphered broadcast scramble key Ks.
[0031]Nowwhile 1st DMUX2 is a means to separate the picture image data and sound data by which waveform shaping was carried outEMMECMand the enciphered broadcast scramble key Ks of the receiving demodulation means 1It is a means to separate the picture image data and sound data of the broadcast descrambling means 5 which were descrambled. 1st DMUX2 is also a means to separate the picture image data and sound data from the reproduction descrambling means 17.
[0032]The EMM decoding means 3 is a means to input EMM from the 1DMUX2to decode EMM with the user ID key Kmand to generate the work key Kw while inputting the user ID key Km.
[0033]The ECM decoding means 4 is a means to input ECM and the enciphered broadcast scramble key Ks from the 1DMUX2to decode ECM with the work key Kwand to restore the broadcast scramble key Ks while inputting the work key Kw from the EMM decoding means 3.
[0034]The broadcast descrambling means 5 inputs the AV information by which scramble was carried out from the 1DMUX2is the broadcast scramble key Ksand is a means to descramble the AV information by which scramble was carried out while it inputs the broadcast scramble key Ks from the ECM decoding means 4.
[0035]The 1st key generating means 6 is a means to generate the record scramble key Kss for carrying out the scramble of the AV information descrambled by the broadcast descrambling means 5 again.
[0036]The record scramble means 7 is a means which inputs the record scramble key Kss from the 1st key generating means 6and carries out the scramble of the AV information with the record scramble key Kss while inputting the AV information from the broadcast descrambling means 5. BelowAV information by which scramble was carried out with the record scramble key Kss is set to Kss (AV information).
[0037]The 2nd key generating means 8 is a means to generate the enciphering key Kc for enciphering the record scramble key Kss which the 1st key generating means 6 generated. The 2nd key generating means 8 shall generate the enciphering key Kc different every dayand makes these different **** Kc Kc1Kc2Kc3and --respectively. enciphering key Kc1Kc2Kc3and -- each presupposes that it is what is discarded in one week.
[0038]While KcFIFO9 is a means to input and store enciphering key Kc1 from the

2nd key generating means 8Kc2Kc3and --It is a means has a timer and discard the enciphering key Kc which passed for one week after the input using the timer to have a first in farce out function.

[0039]The key encoding means 10 is a means to input the enciphering key Kc from KcFIFO9 and to encipher the record scramble key Kss with the enciphering key Kc while inputting the record scramble key Kss from the 1st key generating means 6. Belowthe record scramble key Kss enciphered by the enciphering key Kc is set to Kc (Kss).

[0040]The correspondence relevant information creating means 11 is a means to generate the information on time that enciphering key Kc4 was generatedas information for matching the AV information by which scramble was carried out with the record scramble key Kssand the enciphering key Kc which enciphered the record scramble key Kss.

[0041]MUX12 is a means to input Kss (AV information) from the record scramble means 7Kc (Kss) from the key encoding means 10and the date information from the correspondence relevant information creating means 11and to record them on the videotape 20.

[0042]2nd DMUX13 is a means to input Kss (AV information)Kc (Kss)and date information which were recorded on the videotape 20and to separate them.

[0043]The enciphering key acquisition means 14 is a means to input the date information from the 2DMUX13to specify the enciphering key Kc corresponding to Kss (AV information) which it is going to reproduce based on the date informationand to acquire the specified enciphering key Kc out of KcFIFO9.

[0044]The Kc latch means 15 is a means to input and latch the enciphering key Kc from the enciphering key acquisition means 14and to output to the key decoding means 16.

[0045]The key decoding means 16 is a means to input the enciphering key Kc from the Kc latch means 15to decode Kc (Kss) with the enciphering key Kcand to restore the record scramble key Kss while inputting Kc (Kss) from the 2DMUX13.

[0046]The reproduction descrambling means 17 is a means to input the record scramble key Kss from the key decoding means 16and to descramble Kss (AV information) with the record scramble key Kss while inputting Kss (AV information) from the 2DMUX13.

[0047]The video decoder 18 is a means to decode the picture image data from the 1DMUX2.

[0048]The sound decoder 19 is a means to decode the sound data from the 1DMUX2.

[0049]This invention of claim 1It was considered as the scramble meansand used the 2nd key generating means 8 as the record scramble means 7 and an enciphering key generating meansthe correspondence relevant information creating means 11 was used as a storing meansand MUX12 was used as a recording device as the key encoding means 10 and a correspondence relevant information creating means as KcFIFO9 and a key encoding means. The 1st key generating means 6 was used by this embodiment as a scramble key generating

means of this invention of claim 6. The reproduction descrambling means 17 was used as the key decoding means 16 and a releasing scramble means as the enciphering key acquisition means 14 and a key encryption decoding means as an enciphering key acquisition means of this invention of claim 7.

[0050]Nextoperation of the recording device of such an embodiment of the invention 1 is described.

[0051]The receiving demodulation means 1 Firstthe picture image data of DEJIITARU from a broadcasting stationSound dataEMM (individual information)ECM (program information)and the enciphered broadcast scramble key Ks are inputtedDisorder of the signal wave form of picture image data and sound data is operated orthopedicallyand picture image datasound dataEMMECMand the enciphered broadcast scramble key Ks are outputted to 1st DMUX2.

[0052]Then1st DMUX2 inputs the picture image datathe sound dataEMMECMand the broadcast scramble key Ks from the receiving demodulation means 1it dissociatesand outputs picture image data and sound data (AV information) to the broadcast descrambling means 5. EMM is outputted to the EMM decoding means 3and ECM and the enciphered broadcast scramble key Ks are outputted to the ECM decoding means 4.

[0053]Nextit inputs EMM from the 1DMUX2the EMM decoding means 3 decodes EMM with the user ID key Kmgenerates the work key Kwand outputs it to the ECM decoding means 4 while it inputs the user ID key Km.

[0054]While the ECM decoding means 4 inputs the work key Kw from the EMM decoding means 3ECM and the enciphered broadcast scramble key Ks from the 1DMUX2 are inputtedECM is decoded with the work key Kwencryption of the enciphered broadcast scramble key Ks is restoredand it outputs to the broadcast descrambling means 5. And the broadcast descrambling means 5 inputs the AV information by which scramble was carried out from the 1DMUX2is the broadcast scramble key Ks and descrambles the AV information by which scramble was carried out while it inputs the broadcast scramble key Ks from the ECM decoding means 4. And the broadcast descrambling means 5 outputs the descrambled AV information to the 1DMUX2 or the record scramble means 7. The broadcast descrambling means 5 is outputted to 1st DMUX2when displaying AV information on the display 21 directly in real timeand when making AV information record on the videotape 20it is outputted to the record scramble means 7. Howeverthe AV information recorded on the videotape 20 is not AV information as it is but the data by which scramble was carried out again from the broadcast descrambling means 5.

[0055]Firstthe case where the broadcast descrambling means 5 outputs AV information to 1st DMUX2 is explained.

[0056]In that case1st DMUX2 carries out an AV information input from the broadcast descrambling means 5divides it into picture image data and sound dataoutputs picture image data to the video decoder 18and outputs sound data to the sound decoder 19. thenthe video decoder 18 and the sound decoder 19 -- each decodes the picture image data or sound data from the 1DMUX2and outputs

it to the display 21. And the display 21 displays an image and outputs a sound.
[0057]Nextthe case where the broadcast descrambling means 5 outputs AV information to the record scramble means 7 is explained. That isas mentioned aboveit is a case where AV information is recorded on the videotape 20.
[0058]Firstthe record scramble means 7 inputs the AV information descrambled from the broadcast descrambling means 5.
[0059]And the 1st key generating means 6 generates the record scramble key Kss for carrying out the scramble of the AV information which the record scramble means 7 inputtedand outputs it to the record scramble means 7 and the key encoding means 10.
[0060]Nextthe record scramble means 7 inputs the record scramble key Kss from the 1st key generating means 6and carries out the scramble of the AV information with the record scramble key Kss. That isKss (AV information) is generated. And Kss (AV information) is outputted to the correspondence relevant information creating means 11 and MUX12.
[0061]On the other handthe 2nd key generating means 8 generates the enciphering key Kc for enciphering the record scramble key Kss which the 1st key generating means 6 generated. The enciphering keys Kc which the 2nd key generating means 8 generates shall differ every day. As it supposes here that it is the day of the following explanation when the recording device begins to operate for convenience on January 11998it supposes that it is today which it is at the record time on January 41998 three days after the day and it is shown in the enciphering key Kc list (a) of drawing 2Kc2--the enciphering key Kc generated on January 4 are set to Kc4 for the enciphering key Kc generated in the enciphering key Kc generated on January 1 on Kc January [1 or]2. The enciphering key Kc shall be generated in a similar manner hereafter. As long as there is no noticeoperation of the recording device on January 4 is explained hereafter.
[0062]Nowas shown in the list of drawing 2 (a)from January 1every one enciphering key Kc is already inputted from the 2nd key generating means 8and KcFIFO9 stores it every dayit will store enciphering key Kc1Kc2and Kc3 by January 3and inputs and stores Kc4 on January 4 today. The storing is performed so that the newest enciphering key Kc may always come to the ranking of the top of the list of drawing 2 (a)and an old thing is performed so that ranking may be lowered one by one. KcFIFO9 discards enciphering key Kc1 storedKc2and --after passing for one week since each storing. For examplewhen it becomes as [show / in the list of drawing 2 (b)] on January 9an enciphering key called Kc1 and Kc2 will be discarded and KcFIFO9 will store seven enciphering keys in Kc9Kc8--order of Kc4 and Kc3. That isthe number of the enciphering keys Kc which KcFIFO9 stores is to 7.
[0063]Nextvia KcFIFO9the key encoding means 10 inputs enciphering key Kc4 generated on January 4 it is whose 2nd key generating means 8 at the record timeand enciphers the record scramble key Kss by the enciphering key Kc4 while it inputs the record scramble key Kss from the 1st key generating means 6. That isKc4 (Kss) is generated.

[0064]The correspondence relevant information creating means 11 And Kss (AV information) from the record scramble means 7Kc4 (Kss) from the key encoding means 10 is inputtedand the information on time that the enciphering key Kc4 was generated is generated as information for matching the enciphering key Kc4 and the AV information by which scramble was carried out with the record scramble key Kss enciphered by the enciphering key Kc4. That isthe date information of January 4 is generated.
[0065]ThenMUX12 inputs the date information of Kss (AV information) from the record scramble means 7Kc4 (Kss) from the key encoding means 10and January 4 from the correspondence relevant information creating means 11makes them 1 setand records them on the videotape 20.
[0066]ThusKcn (Kss) corresponding to the enciphering key Kcn (n= 12--) generated on that dayKss (AV information)and the date information of the day will be 1 setand are recorded on the videotape 20 every day.
[0067]Nextoperation of the playback equipment of the embodiment of the invention 1 is described.
[0068]That isthe case where Kss (AV information) recorded on the videotape 20 by the recording device is played is explained.
[0069]Suppose that it is the day of the following explanation when playback equipment plays Kss (AV information) of the videotape 20 for convenience on January 9. And playback equipment shall play Kss (AV information) recorded on the videotape 20 on January 1and Kss (AV information) recorded on the videotape 20 on January 3.
[0070]The case where first playback equipment tends to play Kss (AV information) recorded on the videotape 20 on January 1 is explained.
[0071]First2nd DMUX13 inputs Kss (AV information) recorded on January 1 from the videotape 20Kc1 (Kss)and the date information of January 1separates themand outputs the date information of January 1 to the enciphering key acquisition means 14.
[0072]And the enciphering key acquisition means 14 searches enciphering key Kc1 out of the list of drawing 2 (b) which inputs the date information of the January 1and specifies enciphering key Kc1 based on the date informationand KcFIFO9 stores. Howeversince the enciphering key Kc1 has passed one week or more since generatingit is discarded by KcFIFO9 and does not exist in the list of drawing 2 (b). Thereforethe enciphering key acquisition means 14 cannot acquire enciphering key Kc1. . As a resultit is necessary to descramble the reproduction descrambling means 17using the enciphering key Kc1 indirectly. Even if it becomes impossible to descramble Kss (AV information) recorded on January 1 and the AV information is outputted to the display 21since a decipherment is impossiblethe display 21 cannot output the original image and sound of AV information.
[0073]Nextthe case where playback equipment tends to play Kss (AV information) recorded on the videotape 20 on January 3 is explained.
[0074]First2nd DMUX13 inputs Kss (AV information) recorded on January 3 from the videotape 20Kc3 (Kss)and the date information of January 3separates

themand outputs the date information of January 3 to the enciphering key acquisition means 14.
[0075]Nextthe enciphering key acquisition means 14 inputs the date information of the January 3Based on the date informationenciphering key Kc3 is searched out of the list of drawing 2 (b) which specifies enciphering key Kc3 and KcFIFO9 storesthe enciphering key Kc3 is acquiredand it is outputted to the Kc latch means 15.
[0076]Thenthe Kc latch means 15 inputs enciphering key Kc3and outputs it to the key decoding means 16. 2nd DMUX13 outputs Kc3 (Kss) to the key decoding means 16.
[0077]And while the key decoding means 16 inputs Kc3 (Kss) from the 2DMUX13Enciphering key Kc3 from the Kc latch means 15 is inputtedKc3 (Kss) is decoded by the enciphering key Kc3the record scramble key Kss is restoredand the record scramble key Kss is outputted to the reproduction descrambling means 17. 2nd DMUX13 outputs Kss (AV information) to the key decoding means 16.
[0078]Nextwhile the reproduction descrambling means 17 inputs Kss (AV information) from the 2DMUX13The record scramble key Kss from the key decoding means 16 is inputtedKss (AV information) is descrambled with the record scramble key Kssand the descrambled AV information is outputted to 1st DMUX2.
[0079]And 1st DMUX2 inputs the AV information from the reproduction descrambling means 17divides it into picture image data and sound dataoutputs picture image data to the video decoder 18and outputs sound data to the sound decoder 19. thenthe video decoder 18 and the sound decoder 19 -- each decodes the picture image data or sound data from the 1DMUX2and outputs it to the display 21. And the display 21 displays an image and outputs a sound.
[0080]Thusunless each Kss (AV information) recorded on the videotape 20 has been less than one week since it was recordedit is not eventually played as an original image and sound.
[0081]Although each Kss (AV information) recorded on the videotape 20 presupposed that it will be played if it has been less than one week since it was recorded in Embodiment 1 mentioned aboveIf not restriction of a periodsuch as less than one weekbut the reproduction frequency of each Kss (AV information) is restrictedfor example like 1 time or 3 times and it is not in the restriction reproduction frequencyit is good though not reproduced. That isas shown in drawing 3the playback equipment of this invention is provided with the counter 22When reproduction frequency which the counter 22 checks the reproduction frequency of each Kss (AV information)for exampleit says is 1 time and 3 times and which was restricted is becomeit is good though KcFIFO9 discards the enciphering key Kc corresponding to the Kss (AV information). It is good though restriction of a period and restriction of reproduction frequencysuch as less than one week mentioned aboveare used together.
[0082]In Embodiment 1 mentioned aboveKcFIFO9 presupposed that it discards after one week goes through the stored enciphering key Kc.
HoweverKcFIFO9without discardingeven if one week goes through the stored

enciphering key KcIt is judged whether the day when it keeps stored on and the enciphering key acquisition means 14 tends to reproduce Kss (AV information) is less than one week from generating of the enciphering key KcOr it judges whether it is inside of restricted frequencyand if it is less than inside of less than one week or restricted frequencyit is good though the enciphering key Kc corresponding to Kss (AV information) which it is going to reproduce is acquirable from KcFIFO9. Thereforein this case in this invention of claim 8. As a scramble meansas the record scramble means 7 and an enciphering key generating means. MUX12 will correspond as the correspondence relevant information creating means 11 and a recording device as the key encoding means 10 and a correspondence relevant information creating means as KcFIFO9 and a key encoding means as the 2nd key generating means 8 and a storing meansrespectively. In this invention of claim 12the reproduction descrambling means 17 will correspond as the key decoding means 16 and a releasing scramble means as the enciphering key acquisition means 14 and a key encryption decoding means as an enciphering key acquisition meansrespectively.

[0083]In Embodiment 1 mentioned abovethe 1st key generating means 6 presupposed that the record scramble key Kss for carrying out the scramble of the AV information which the record scramble means 7 inputted is generated. Howeveras shown in drawing 4the recording device of this invention is not provided with the 1st key generating means 6but the record scramble means 7The broadcast scramble key Ks sent is inputted via the broadcast descrambling means 5 from a broadcasting stationand it is the broadcast scramble key Ksor is what processed the broadcast scramble key Ksand it is good though the scramble of the AV information is carried out. In that casefrom the record scramble means 7the key encoding means 10 inputs the broadcast scramble key Ks or the thing which processed the broadcast scramble key Ksand enciphers it with the enciphering key Kc.

[0084]In Embodiment 1 mentioned abovethe record scramble means 7 presupposed that the scramble of the AV information is carried out with the record scramble key Kss from the 1st key generating means 6. Howeveras shown in drawing 5the recording device of this invention is not provided with the 1st key generating means 6 and the key encoding means 10but the record scramble means 7It is goodthough the enciphering key Kc from the 2nd key generating means 8 is inputted via KcFIFO9the enciphering key Kc is used as the record scramble key Kc and the scramble of the AV information is carried out with the record scramble key Kc. In this casethe AV information by which scramble was carried out with the record scramble key Kci.e.Kc(AV information)and the record scramble key Kc are recorded on the videotape 20. In that casethe playback equipment of this invention will be provided with the key decoding means 16as shown in drawing 5. Thereforewhen it is going to reproduce Kc (AV information)the scramble key acquisition means 23 specifies the corresponding record scramble key Kcand acquires it out of KcFIFO9. And while the playback descrambling means 17 inputs Kc (AV information) from the videotape 20 via 2nd DMUX13The record scramble

key Kc from the scramble key acquisition means 23 is inputted via the Kc latch means 15and Kc (AV information) is descrambled with the record scramble key Kc. Thereforeby this invention of claims 15 and 20in this case that is. 1st DMUX2 will correspond as the correspondence relevant information creating means 11 and a recording device as the record scramble means 7 and a correspondence relevant information creating means as KcFIFO9 and a scramble means as the 2nd key generating means 8 and a storing means as a scramble key generating meansrespectively. In this invention of claims 19 and 22the reproduction descrambling means 17 will correspond as the scramble key acquisition means 23 and a releasing scramble means as a scramble key acquisition meansrespectively.

[0085]The recording device of Embodiment 1 mentioned above is provided with the charging means 24 as shown in drawing 6A user is burdened with the predetermined fee collection to the record when recording Kss (AV information) on the videotape 20When a predetermined fee is beforehand paid to a broadcasting station etc. by the useror only when recording at least and a predetermined fee is paidthough Kss (AV information) is recorded on the videotape 20it is good. Even if it is not arranged at the position shown in drawing 6though the charging means 24 is arranged between the key encoding means 10 and MUX12it is good. what burdens a user with the predetermined fee collection to the record in short when the charging means 24 records Kss (AV information) on the videotape 20 -- it is even -- What is necessary is just to carry out. may an arrangement place be any place?

[0086]Although it presupposed that it will be discarded if each enciphering key Kc passes for one week since generating in Embodiment 1 mentioned abovethe time discarded may not be limited after one-week progress from generatingand may be after [one day] progressmay be after [three day] progressor may be after 12-hour progress. lapse of period predetermined [from generating] in short in each enciphering key Kc -- if it carries outit will discard -- even having -- what is necessary is just to carry out

[0087]In Embodiment 1 mentioned abovealthough the enciphering key Kc in which one differs at a time is generated every dayeven if it is the same daythough the 2nd key generating means 8 generates the enciphering key Kc different every several hoursit is good. [of the 2nd key generating means 8] It is goodthough the enciphering key Kc is generated whenever it records Kss (AV information) of a predetermined program on the videotape 20. That isit is good though the enciphering key Kc is generated for every end of the recording from one recording start each time. In shortthe 2nd key generating means 8 has only to generate the enciphering key Kc for enciphering the record scramble key Kss of Kss (AV information) which it is going to record.

[0088]Although the date information at the time of the enciphering key Kc being generated was used as correspondence relevant information of this invention in Embodiment 1 mentioned aboveThe time as whichas for the correspondence relevant information of this inventionthe record scramble means 7 inputted AV informationThe time to which the record scramble means 7 carried out the

scramble of the AV information with the record scramble key KssThe time at which the 2nd key generating means 8 generated the enciphering key Kcthe time in which KcFIFO9 stored the enciphering key KcIt may be the information on the time as which the key encoding means 10 enciphered the record scramble key Kss with the enciphering key Kcor the time at which MUX12 recorded Kss (AV information) on the videotape 20. Or it may be the information on the time at the time of the enciphering key Kc mentioned above being generatedthe time as which the record scramble means 7 inputted AV informationetc. and the time which is going to reproduce AV information. In that casebased on each enciphering key Kc of the enciphering key Kc list of drawing 2 lowering ranking every daythe difference of two time will be taken into consideration and the enciphering key Kc will be acquired. Or time at the time of the enciphering key Kc which the correspondence relevant information of this invention mentioned above being generatedtime as which the record scramble means 7 inputted AV informationetc.Based on the time which is going to reproduce AV informationit may be the number information etc. of the enciphering key Kc list of drawing 2 in which it was taken into consideration that each enciphering key Kc of the enciphering key Kc list of drawing 2 lowers ranking every day.

[0089]In Embodiment 1 mentioned abovealthough the videotape 20 as a recording medium was useda recording medium may be not only the videotape 20 but a hard disk.

[0090]Although the record scramble key Kss for the 1st key generating means 6 to carry out the scramble of the AV information is generated in Embodiment 1 mentioned abovethough the record scramble key Kss is updated in short periodssuch as tens of secondsso that it cannot decode easily for exampleit is good.

[0091]The recording device or playback equipment mentioned aboveThe predetermined period of one week passes since generating of the enciphering key Kcand when Kss (AV information) corresponding to the enciphering key Kc is not once reproduced before the enciphering key Kc is discarded or use becomes improperit may have a means to notify a user of information to that effect.

[0092]

[Effect of the Invention]This invention can record AV information on a recording mediumand can provide the recording device and playback equipment which observe during the effective regeneration phase of the AV informationand restriction of effective reproduction frequency so that clearly from the place explained above.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]The block diagram of the recording device of the embodiment of the invention 1and playback equipment

[Drawing 2]The figure showing an example of the enciphering key Kc list used for the recording device and playback equipment of the embodiment of the invention 1
[Drawing 3]A different block diagram of the recording device of this inventionand playback equipment from drawing 1
[Drawing 4]A block diagram of the recording device of this inventionand playback equipment which is different in drawing 1 or 3
[Drawing 5]The block diagram of the recording device of drawing 1 and this invention which is different in 3 or 4and playback equipment
[Drawing 6]The block diagram of the recording device of drawing 1 and this invention which is different in 34or 5and playback equipment
[Drawing 7]The block diagram of conventional recording playback equipment
[Description of Notations]
1 Receiving demodulation means
2 The 1st DMUX
3 EMM decoding means
4 ECM decoding means
5 Broadcast descrambling means
6 The 1st key generating means
7 Record scramble means
8 The 2nd key generating means
9 KcFIFO
10 Key encoding means
11 Correspondence relevant information creating means
12 MUX
13 The 2nd DMUX
14 Enciphering key acquisition means
15 Kc latch means
16 Key decoding means
17 Reproduction descrambling means
18 Video decoder
19 Sound decoder
20 Videotape
21 Display
22 Counter
23 Scramble key acquisition means
24 Charging means

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－232776

(43)公開日　平成11年(1999)８月27日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｄ
Ｇ１１Ｂ　20/00		Ｇ１１Ｂ　20/00	Ｚ
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｚ
Ｈ０４Ｎ　5/91		Ｈ０４Ｎ　5/91	Ｐ

審査請求　未請求　請求項の数27　ＯＬ　（全 16 頁）　最終頁に続く

(21)出願番号　特願平10－27572

(22)出願日　平成10年(1998)２月９日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　山田　正純
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　飯塚　裕之
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　武知　秀明
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(74)代理人　弁理士　松田　正道

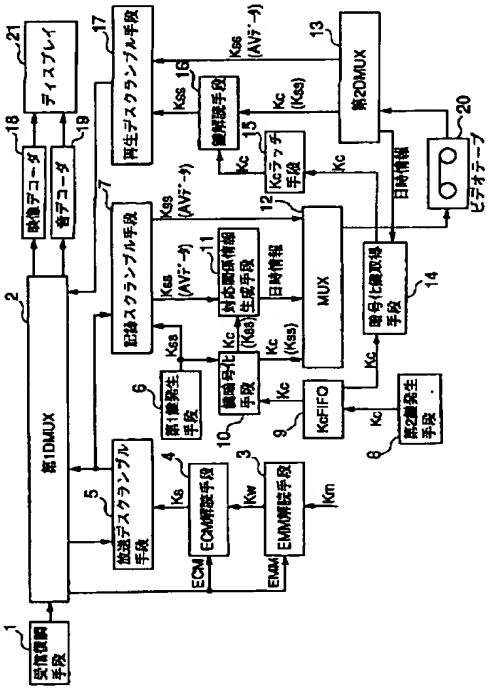
最終頁に続く

(54)【発明の名称】　録画装置および再生装置

(57)【要約】

【課題】従来の録画再生装置は、ＡＶデータを記録媒体に記録すると、そのＡＶデータの有効再生期間や有効再生回数の制限を守らないという課題があった。

【解決手段】スクランブル鍵ＫｓｓでＡＶデータをスクランブルする記録スクランブル手段７と、スクランブル鍵Ｋｓｓを暗号化するための暗号化鍵Ｋｃを発生する第２鍵発生手段８と、第２鍵発生手段８からの暗号化鍵Ｋｃを格納し、その後、その暗号化鍵Ｋｃが所定の条件に合えば、その暗号化鍵Ｋｃを消去するＫｃＦＩＦＯ９と、暗号化鍵Ｋｃでスクランブル鍵Ｋｓｓを暗号化する鍵暗号化手段１０と、暗号化鍵Ｋｃが発生された日時の情報を生成する対応関係情報生成手段１１と、スクランブルされた映像および／または音のデータ、暗号化されたスクランブル鍵Ｋｓｓ、および、日時情報を入力し、それらをビデオテープ２０に記録するＭＵＸ１２とを備える。



【特許請求の範囲】
【請求項１】映像および／または音のデータを入力するとともに、前記映像および／または音のデータをスクランブルするためのスクランブル鍵を入力し、そのスクランブル鍵で前記映像および／または音のデータをスクランブルするスクランブル手段と、
前記スクランブル鍵を暗号化するための暗号化鍵を発生する暗号化鍵発生手段と、
前記暗号化鍵発生手段が発生した暗号化鍵を格納し、その後、その暗号化鍵が所定の条件に合えば、その暗号化鍵を消去する格納手段と、
前記スクランブル手段からのスクランブル鍵を入力するとともに、前記暗号化鍵発生手段からの前記暗号化鍵を入力し、その暗号化鍵で前記スクランブル鍵を暗号化する鍵暗号化手段と、
前記スクランブル鍵によりスクランブルされた映像および／または音のデータと、そのスクランブル鍵を暗号化した暗号化鍵との対応関係情報を生成する対応関係情報生成手段と、
前記スクランブル手段からのスクランブルされた映像および／または音のデータ、前記鍵暗号化手段からの暗号化されたスクランブル鍵、および、前記対応関係情報生成手段からの対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを備えたことを特徴とする録画装置。
【請求項２】前記所定の条件とは、前記暗号化鍵が格納された後、所定の時間を超えることを意味することを特徴とする請求項１記載の録画装置。
【請求項３】前記対応関係情報とは、前記スクランブル手段が前記映像および／または音のデータを入力した日時、前記スクランブル手段が前記スクランブル鍵で前記映像および／または音のデータをスクランブルした日時、前記暗号化鍵発生手段が前記暗号化鍵を発生した日時、前記格納手段が前記暗号化鍵を格納した日時、前記鍵暗号化手段が前記暗号化鍵で前記スクランブル鍵を暗号化した日時、または、前記記録手段が前記所定の記録媒体に前記スクランブルされた映像および／または音のデータを記録した日時で対応付けられた情報であることを特徴とする請求項１または２記載の録画装置。
【請求項４】前記所定の条件とは、前記スクランブルされた映像および／または音のデータの再生のさいに、前記暗号化鍵の利用された回数が、所定の回数を超えることを意味することを特徴とする請求項１記載の録画装置。
【請求項５】前記スクランブル鍵を発生するスクランブル鍵発生手段を備え、前記スクランブル手段は、前記スクランブル鍵発生手段から前記スクランブル鍵を入力することを特徴とする請求項１から４のいずれかに記載の録画装置。
【請求項６】前記スクランブル手段は、放送局からの前記スクランブル鍵を入力し、そのスクランブル鍵を利用することを特徴とする請求項１から４のいずれかに記載の録画装置。
【請求項７】請求項１から６のいずれかに記載の所定の記録媒体からの、請求項１から６のいずれかに記載の前記対応関係情報を入力し、その対応関係情報に基づいて、再生しようとするスクランブルされた映像および／または音のデータに対応する暗号化鍵を特定し、請求項１から６のいずれかに記載の格納手段のなかの前記暗号化鍵を検索して取得する暗号化鍵取得手段と、
前記所定の記録媒体からの、前記再生しようとするスクランブルされた映像および／または音のデータに対応する、暗号化されたスクランブル鍵を入力するとともに、前記暗号化鍵取得手段からの暗号化鍵を入力し、その暗号化鍵で前記暗号化された前記スクランブル鍵の暗号化を解く鍵暗号化解読手段と、
前記所定の記録媒体からの、スクランブルされた映像および／または音のデータを入力するとともに、前記鍵暗号化解読手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記スクランブルされた映像および／または音のデータのスクランブルを解除するスクランブル解除手段とを備えたことを特徴とする再生装置。
【請求項８】映像および／または音のデータを入力するとともに、前記映像および／または音のデータをスクランブルするためのスクランブル鍵を入力し、そのスクランブル鍵で前記映像および／または音のデータをスクランブルするスクランブル手段と、
前記スクランブル鍵を暗号化するための暗号化鍵を発生する暗号化鍵発生手段と、
前記暗号化鍵発生手段が発生した暗号化鍵を格納する格納手段と、
前記スクランブル手段からのスクランブル鍵を入力するとともに、前記暗号化鍵発生手段からの前記暗号化鍵を入力し、その暗号化鍵で前記スクランブル鍵を暗号化する鍵暗号化手段と、
前記スクランブル鍵によりスクランブルされた映像および／または音のデータと、そのスクランブル鍵を暗号化した暗号化鍵との対応関係情報を生成する対応関係情報生成手段と、
前記スクランブル手段からのスクランブルされた映像および／または音のデータ、前記鍵暗号化手段からの暗号化されたスクランブル鍵、および、前記対応関係情報生成手段からの対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを備えたことを特徴とする録画装置。
【請求項９】前記対応関係情報とは、前記スクランブル手段が前記映像および／または音のデータを入力した日時、前記スクランブル手段が前記スクランブル鍵で前記映像および／または音のデータをスクランブルした日時、前記暗号化鍵発生手段が前記暗号化鍵を発生した日

時、前記格納手段が前記暗号化鍵を格納した日時、前記鍵暗号化手段が前記暗号化鍵で前記スクランブル鍵を暗号化した日時、または、前記記録手段が前記所定の記録媒体に前記スクランブルされた映像および／または音のデータを記録した日時で対応付けられた情報であることを特徴とする請求項８記載の録画装置。

【請求項１０】前記スクランブル鍵を発生するスクランブル鍵発生手段を備え、前記スクランブル手段は、前記スクランブル鍵発生手段から前記スクランブル鍵を入力することを特徴とする請求項８または９記載の録画装置。

【請求項１１】前記スクランブル手段は、放送局からの前記スクランブル鍵を入力し、そのスクランブル鍵を利用することを特徴とする請求項８または９記載の録画装置。

【請求項１２】請求項８から１１のいずれかに記載の所定の記録媒体からの、請求項８から１１のいずれかに記載の対応関係情報を入力し、その対応関係情報に基づいて、再生しようとするスクランブルされた映像および／または音のデータに対応する暗号化鍵を特定し、さらに、その暗号化鍵が所定の条件に合うかどうかを判定し、合致する場合は、その暗号化鍵を、請求項８から１１のいずれかに記載の格納手段から取り出し、合致しない場合は、その暗号化鍵を前記格納手段から取り出さない暗号化鍵取得手段と、

前記所定の記録媒体からの、前記再生しようとするスクランブルされた映像および／または音のデータに対応する、暗号化されたスクランブル鍵を入力するとともに、前記暗号化鍵取得手段からの暗号化鍵を入力し、その暗号化鍵で前記暗号化された前記スクランブル鍵の暗号化を解く鍵暗号化解読手段と、

前記所定の記録媒体からの、スクランブルされた映像および／または音のデータを入力するとともに、前記鍵暗号化解読手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記スクランブルされた映像および／または音のデータのスクランブルを解除するスクランブル解除手段とを備えたことを特徴とする再生装置。

【請求項１３】前記所定の条件とは、請求項８から１１のいずれかに記載の格納手段に、前記暗号化鍵が格納された後、所定の時間を超えることを意味することを特徴とする請求項１２記載の再生装置。

【請求項１４】前記所定の条件とは、前記スクランブルされた映像および／または音のデータの再生のさいに、前記暗号化鍵の利用された回数が、所定の回数を超えることを意味することを特徴とする請求項１２記載の再生装置。

【請求項１５】映像および／または音のデータをスクランブルするためのスクランブル鍵を発生するスクランブル鍵発生手段と、

前記スクランブル鍵発生手段が発生したスクランブル鍵を格納し、その後、そのスクランブル鍵が所定の条件に合えば、そのスクランブル鍵を消去する格納手段と、

前記映像および／または音のデータを入力するとともに、前記スクランブル鍵発生手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記映像および／または音のデータをスクランブルするスクランブル手段と、

前記スクランブル鍵によりスクランブルされた映像および／または音のデータと、そのスクランブル鍵との対応関係情報を生成する対応関係情報生成手段と、

前記スクランブル手段からのスクランブルされた映像および／または音のデータ、および、前記対応関係情報生成手段からの対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを備えたことを特徴とする録画装置。

【請求項１６】前記所定の条件とは、前記スクランブル鍵が格納された後、所定の時間を超えることを意味することを特徴とする請求項１５記載の録画装置。

【請求項１７】前記対応関係情報とは、前記スクランブル手段が前記映像および／または音のデータを入力した日時、前記スクランブル手段が前記スクランブル鍵で前記映像および／または音のデータをスクランブルした日時、前記スクランブル鍵発生手段が前記スクランブル鍵を発生した日時、前記格納手段が前記スクランブル鍵を格納した日時、または、前記記録手段が前記所定の記録媒体に前記スクランブルされた映像および／または音のデータを記録した日時で対応付けられた情報であることを特徴とする請求項１５または１６記載の録画装置。

【請求項１８】前記所定の条件とは、前記スクランブルされた映像および／または音のデータの再生のさいに、前記暗号化鍵の利用された回数が、所定の回数を超えることを意味することを特徴とする請求項１５記載の録画装置。

【請求項１９】請求項１５から１８のいずれかに記載の所定の記録媒体からの、請求項１５から１８のいずれかに記載の対応関係情報を入力し、その対応関係情報に基づいて、再生しようとするスクランブルされた映像および／または音のデータに対応するスクランブル鍵を特定し、請求項１５から１８のいずれかに記載の格納手段のなかの前記スクランブル鍵を検索して取得するスクランブル鍵取得手段と、

前記所定の記録媒体からの、前記再生しようとするスクランブルされた映像および／または音のデータに対応する、前記スクランブルされた映像および／または音のデータを入力するとともに、前記スクランブル鍵取得手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記スクランブルされた映像および／または音のデータのスクランブルを解除するスクランブル解除手段とを備えたことを特徴とする再生装置。

【請求項２０】映像および／または音のデータをスクランブルするためのスクランブル鍵を発生するスクランブ

ル鍵発生手段と、
前記スクランブル鍵発生手段が発生したスクランブル鍵を格納する格納手段と、
前記映像および／または音のデータを入力するとともに、前記スクランブル鍵発生手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記映像および／または音のデータをスクランブルするスクランブル手段と、
前記スクランブル鍵によりスクランブルされた映像および／または音のデータと、そのスクランブル鍵との対応関係情報を生成する対応関係情報生成手段と、
前記スクランブル手段からのスクランブルされた映像および／または音のデータ、および、前記対応関係情報生成手段からの対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを備えたことを特徴とする録画装置。
【請求項２１】前記対応関係情報とは、前記スクランブル手段が前記映像および／または音のデータを入力した日時、前記スクランブル手段が前記スクランブル鍵で前記映像および／または音のデータをスクランブルした日時、前記スクランブル鍵発生手段が前記スクランブル鍵を発生した日時、前記格納手段が前記スクランブル鍵を格納した日時、または、前記記録手段が前記所定の記録媒体に前記スクランブルされた映像および／または音のデータを記録した日時で対応付けられた情報であることを特徴とする請求項２０記載の録画装置。
【請求項２２】請求項２０または２１記載の所定の記録媒体からの、請求項２０または２１記載の対応関係情報を入力し、その対応関係情報に基づいて、再生しようとするスクランブルされた映像および／または音のデータに対応するスクランブル鍵を特定し、さらに、そのスクランブル鍵が所定の条件に合うかどうかを判定し、合致する場合は、そのスクランブル鍵を、請求項２０または２１記載の格納手段から取り出し、合致しない場合は、そのスクランブル鍵を前記格納手段から取り出さないスクランブル鍵取得手段と、
前記所定の記録媒体からの、前記再生しようとするスクランブルされた映像および／または音のデータに対応する、スクランブルされた映像および／または音のデータを入力するとともに、前記スクランブル鍵取得手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記スクランブルされた映像および／または音のデータのスクランブルを解除するスクランブル解除手段とを備えたことを特徴とする再生装置。
【請求項２３】前記所定の条件とは、請求項２０または２１記載の格納手段に、前記スクランブル鍵が格納された後、所定の時間を超えることを意味することを特徴とする請求項２２記載の再生装置。
【請求項２４】前記所定の条件とは、前記スクランブルされた映像および／または音のデータの再生のさいに、前記スクランブル鍵の利用された回数が、所定の回数を超えることを意味することを特徴とする請求項２２記載の再生装置。
【請求項２５】前記記録手段が前記スクランブル手段からのスクランブルされた映像および／または音のデータを、前記所定の記録媒体に記録するさい、前記データの記録に対する課金を課す課金手段を備えたことを特徴とする請求項１から６のいずれか、または、請求項８から１１のいずれか、または、請求項１５から１８のいずれか、または、請求項２０から２１のいずれかに記載の録画装置。
【請求項２６】前記所定の記録媒体は、ビデオテープであることを特徴とする請求項１から６のいずれか、または、請求項８から１１のいずれか、または、請求項１５から１８のいずれか、または、請求項２０から２１のいずれかに記載の録画装置。
【請求項２７】前記所定の記録媒体は、ハードディスクであることを特徴とする請求項１から６のいずれか、または、請求項８から１１のいずれか、または、請求項１５から１８のいずれか、または、請求項２０から２１のいずれかに記載の録画装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、著作権等により再生についての期間や回数が制限された、映像および／または音のデータを録画する録画装置と、その映像および／または音のデータを再生する再生装置とに関するものである。
【０００２】
【従来の技術】現在、著作権保護の対象となっている映画や音楽等のＡＶデータは、ビデオテープ等に格納されている。ユーザは、そのようなビデオテープ等を有料で貸し出すレンタル店を通じて、例えば１週間というような所定の期間のみビデオテープ等を借り、それを再生することによって、映画や音楽等を鑑賞することができる。
【０００３】他方、上述したビデオテープ等のレンタルのシステムとは別に、ディジタル技術や暗号化技術の進歩等から、放送局からの映画や音楽等の番組を通信衛星を介して入力し、その番組をスクランブルしてビデオテープ等に録画し、再生する録画再生装置として、以下のものが考えられている。
【０００４】図７に、このような従来の録画再生装置のブロック図を示す。
【０００５】受信復調手段１は、衛星放送の、デジィタルの映像データ、音データ、ＥＭＭ（個別情報）、ＥＣＭ（番組情報）および暗号化された放送スクランブル鍵Ｋｓを入力し、第１ＤＭＵＸ２は、受信復調手段１からの映像データ、音データ、ＥＭＭ、ＥＣＭおよび放送スクランブル鍵Ｋｓを分離する。そして、ＥＭＭ解読手段３は、第１ＤＭＵＸ２からのＥＭＭを入力するととも

に、ユーザＩＤ鍵Ｋｍを入力し、そのユーザＩＤ鍵ＫｍでＥＭＭを解読してワーク鍵Ｋｗを生成する。ＥＣＭ解読手段４は、ＥＭＭ解読手段３からのワーク鍵Ｋｗを入力するとともに、第１ＤＭＵＸ２からのＥＣＭおよび暗号化された放送スクランブル鍵Ｋｓを入力し、ワーク鍵ＫｗでＥＣＭを解読して、暗号化された放送スクランブル鍵Ｋｓを復元する。

【０００６】その後、放送デスクランブル手段５は、ＥＣＭ解読手段４からの放送スクランブル鍵Ｋｓを入力するとともに、第１ＤＭＵＸ２からの、スクランブルされたＡＶデータを入力し、放送スクランブル鍵Ｋｓで、スクランブルされたＡＶデータをデスクランブルする。そして、放送デスクランブル手段５は、デスクランブルされたＡＶデータを、リアルタイムでＡＶデータを直接ディスプレイ２１に表示させる場合に第１ＤＭＵＸ２に出力し、また、ビデオテープ２０にＡＶデータを記録させる場合に記録スクランブル手段７に出力する。

【０００７】放送デスクランブル手段５がＡＶデータを第１ＤＭＵＸ２に出力する場合、第１ＤＭＵＸ２は、放送デスクランブル手段５からのＡＶデータを映像データと音データに分離して、映像データを映像デコーダ１８に出力し、音データを音デコーダ１９に出力する。そして、映像デコーダ１８および音デコーダ１９それぞれは、第１ＤＭＵＸ２からの映像データまたは音データを復号し、ディスプレイ２１は、映像を表示し音を出力する。

【０００８】他方、放送デスクランブル手段５がＡＶデータを記録スクランブル手段７に出力する場合、記録スクランブル手段７は、放送デスクランブル手段５からのＡＶデータを入力するとともに、第１鍵発生手段６からの記録スクランブル鍵Ｋｓｓを入力し、その記録スクランブル鍵Ｋｓｓで、ＡＶデータをスクランブルする。その記録スクランブル鍵Ｋｓｓによりスクランブルされた ＡＶデータをＫｓｓ（ＡＶデータ）とする。

【０００９】それとともに、第２鍵発生手段８は、記録スクランブル鍵Ｋｓｓを暗号化するための暗号化鍵Ｋｃを発生し、鍵暗号化手段１０は、第１鍵発生手段６からの記録スクランブル鍵Ｋｓｓを入力するとともに、第２鍵発生手段８からの暗号化鍵Ｋｃを入力し、その暗号化鍵Ｋｃで記録スクランブル鍵Ｋｓｓを暗号化する。その暗号化鍵Ｋｃにより暗号化された記録スクランブル鍵ＫｓｓをＫｃ（Ｋｓｓ）とする。

【００１０】そして、ＭＵＸ１２は、記録スクランブル手段７からのＫｓｓ（ＡＶデータ）と、鍵暗号化手段１０からのＫｃ（Ｋｓｓ）とを入力し、それらをビデオテープ２０に記録する。

【００１１】そのビデオテープ２０に記録されたＫｓｓ（ＡＶデータ）を再生する場合、先ず、第２ＤＭＵＸ１３は、ビデオテープ２０からのＫｓｓ（ＡＶデータ）と、Ｋｃ（Ｋｓｓ）とを入力して分離する。そして、鍵解読手段１６は、第２ＤＭＵＸ１３からのＫｃ（Ｋｓｓ）を入力するとともに、第２鍵発生手段８からの暗号化鍵Ｋｃを入力し、その暗号化鍵ＫｃでＫｃ（Ｋｓｓ）を解読して、記録スクランブル鍵Ｋｓｓを復元する。さらに、再生デスクランブル手段１７は、第２ＤＭＵＸ１３からのＫｓｓ（ＡＶデータ）を入力するとともに、鍵解読手段１６からの記録スクランブル鍵Ｋｓｓを入力し、その記録スクランブル鍵ＫｓｓでＫｓｓ（ＡＶデータ）をデスクランブルして、そのデスクランブルされたＡＶデータを第１ＤＭＵＸ２に出力する。

【００１２】最後に、第１ＤＭＵＸ２に出力されたＡＶデータは、リアルタイムにおける、ディスプレイ２１の映像表示および音出力と同様にして、ディスプレイ２１によって映像として表示され、また、音として出力される。

【００１３】

【発明が解決しようとする課題】ところで、上述したビデオテープ等のレンタルのシステムは、これからの多チャンネルディジタル放送時代においても、ユーザがその都度レンタル店に出向いてビデオテープ等を借りなければならないという点など、ユーザにとって相変わらず手間がかかり不便である。

【００１４】また、上述した従来の録画再生装置では、ＡＶデータを一度ビデオテープ２０に記録すると、第２鍵発生手段８からの暗号化鍵Ｋｃを利用しさえすれば、そのＡＶデータは、いつでも、また、何度でも再生され、ディスプレイ２１によって映像および／または音として出力される。このように、従来の録画再生装置では、映画や音楽等の著作権保護の対象となっているＡＶデータの有効再生期間や有効再生回数には制限がないということになる。例えば、劇場放映直後の映画のように、特別な価値を有するＡＶデータが上述したような、再生の期間や回数について制限のない録画再生装置によって記録媒体に記録されると、そのＡＶデータの価値は半減する。つまり、放送局は、そのような特別な価値を有するＡＶデータを安心して放送することができない。

【００１５】本発明は、このような従来の録画再生装置は、ＡＶデータを記録媒体に記録すると、そのＡＶデータの有効再生期間や有効再生回数の制限を守らないという課題を考慮し、ＡＶデータを記録媒体に記録し、そのＡＶデータの有効再生期間や有効再生回数の制限を遵守する録画装置および再生装置を提供することを目的とするものである。

【００１６】

【課題を解決するための手段】請求項１の本発明は、映像および／または音のデータを入力するとともに、前記映像および／または音のデータをスクランブルするためのスクランブル鍵を入力し、そのスクランブル鍵で前記映像および／または音のデータをスクランブルするスクランブル手段と、前記スクランブル鍵を暗号化するため

の暗号化鍵を発生する暗号化鍵発生手段と、前記暗号化鍵発生手段が発生した暗号化鍵を格納し、その後、その暗号化鍵が所定の条件に合えば、その暗号化鍵を消去する格納手段と、前記スクランブル手段からのスクランブル鍵を入力するとともに、前記暗号化鍵発生手段からの前記暗号化鍵を入力し、その暗号化鍵で前記スクランブル鍵を暗号化する鍵暗号化手段と、前記スクランブル鍵によりスクランブルされた映像および／または音のデータと、そのスクランブル鍵を暗号化した暗号化鍵との対応関係情報を生成する対応関係情報生成手段と、前記スクランブル手段からのスクランブルされた映像および／または音のデータ、前記鍵暗号化手段からの暗号化されたスクランブル鍵、および、前記対応関係情報生成手段からの対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを備えたことを特徴とする録画装置である。

【００１７】請求項７の本発明は、請求項１から６のいずれかに記載の所定の記録媒体からの、請求項１から６のいずれかに記載の前記対応関係情報を入力し、その対応関係情報に基づいて、再生しようとするスクランブルされた映像および／または音のデータに対応する暗号化鍵を特定し、請求項１から６のいずれかに記載の格納手段のなかの前記暗号化鍵を検索して取得する暗号化鍵取得手段と、前記所定の記録媒体からの、前記再生しようとするスクランブルされた映像および／または音のデータに対応する、暗号化されたスクランブル鍵を入力するとともに、前記暗号化鍵取得手段からの暗号化鍵を入力し、その暗号化鍵で前記暗号化された前記スクランブル鍵の暗号化を解く鍵暗号化解読手段と、前記所定の記録媒体からの、スクランブルされた映像および／または音のデータを入力するとともに、前記鍵暗号化解読手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記スクランブルされた映像および／または音のデータのスクランブルを解除するスクランブル解除手段とを備えたことを特徴とする再生装置である。

【００１８】請求項８の本発明は、映像および／または音のデータを入力するとともに、前記映像および／または音のデータをスクランブルするためのスクランブル鍵を入力し、そのスクランブル鍵で前記映像および／または音のデータをスクランブルするスクランブル手段と、前記スクランブル鍵を暗号化するための暗号化鍵を発生する暗号化鍵発生手段と、前記暗号化鍵発生手段が発生した暗号化鍵を格納する格納手段と、前記スクランブル手段からのスクランブル鍵を入力するとともに、前記暗号化鍵発生手段からの前記暗号化鍵を入力し、その暗号化鍵で前記スクランブル鍵を暗号化する鍵暗号化手段と、前記スクランブル鍵によりスクランブルされた映像および／または音のデータと、そのスクランブル鍵を暗号化した暗号化鍵との対応関係情報を生成する対応関係情報生成手段と、前記スクランブル手段からのスクランブルされた映像および／または音のデータ、前記鍵暗号化手段からの暗号化されたスクランブル鍵、および、前記対応関係情報生成手段からの対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを備えたことを特徴とする録画装置である。

【００１９】請求項１２の本発明は、請求項８から１１のいずれかに記載の所定の記録媒体からの、請求項８から１１のいずれかに記載の対応関係情報を入力し、その対応関係情報に基づいて、再生しようとするスクランブルされた映像および／または音のデータに対応する暗号化鍵を特定し、さらに、その暗号化鍵が所定の条件に合うかどうかを判定し、合致する場合は、その暗号化鍵を、請求項８から１１のいずれかに記載の格納手段から取り出し、合致しない場合は、その暗号化鍵を前記格納手段から取り出さない暗号化鍵取得手段と、前記所定の記録媒体からの、前記再生しようとするスクランブルされた映像および／または音のデータに対応する、暗号化されたスクランブル鍵を入力するとともに、前記暗号化鍵取得手段からの暗号化鍵を入力し、その暗号化鍵で前記暗号化された前記スクランブル鍵の暗号化を解く鍵暗号化解読手段と、前記所定の記録媒体からの、スクランブルされた映像および／または音のデータを入力するとともに、前記鍵暗号化解読手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記スクランブルされた映像および／または音のデータのスクランブルを解除するスクランブル解除手段とを備えたことを特徴とする再生装置である。

【００２０】請求項１５の本発明は、映像および／または音のデータをスクランブルするためのスクランブル鍵を発生するスクランブル鍵発生手段と、前記スクランブル鍵発生手段が発生したスクランブル鍵を格納し、その後、そのスクランブル鍵が所定の条件に合えば、そのスクランブル鍵を消去する格納手段と、前記映像および／または音のデータを入力するとともに、前記スクランブル鍵発生手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記映像および／または音のデータをスクランブルするスクランブル手段と、前記スクランブル鍵によりスクランブルされた映像および／または音のデータと、そのスクランブル鍵との対応関係情報を生成する対応関係情報生成手段と、前記スクランブル手段からのスクランブルされた映像および／または音のデータ、および、前記対応関係情報生成手段からの対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを備えたことを特徴とする録画装置である。

【００２１】請求項１９の本発明は、請求項１５から１８のいずれかに記載の所定の記録媒体からの、請求項１５から１８のいずれかに記載の対応関係情報を入力し、その対応関係情報に基づいて、再生しようとするスクランブルされた映像および／または音のデータに対応する

スクランブル鍵を特定し、請求項１５から１８のいずれかに記載の格納手段のなかの前記スクランブル鍵を検索して取得するスクランブル鍵取得手段と、前記所定の記録媒体からの、前記再生しようとするスクランブルされた映像および／または音のデータに対応する、前記スクランブルされた映像および／または音のデータを入力するとともに、前記スクランブル鍵取得手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記スクランブルされた映像および／または音のデータのスクランブルを解除するスクランブル解除手段とを備えたことを特徴とする再生装置である。

【００２２】請求項２０の本発明は、映像および／または音のデータをスクランブルするためのスクランブル鍵を発生するスクランブル鍵発生手段と、前記スクランブル鍵発生手段が発生したスクランブル鍵を格納する格納手段と、前記映像および／または音のデータを入力するとともに、前記スクランブル鍵発生手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記映像および／または音のデータをスクランブルするスクランブル手段と、前記スクランブル鍵によりスクランブルされた映像および／または音のデータと、そのスクランブル鍵との対応関係情報を生成する対応関係情報生成手段と、前記スクランブル手段からのスクランブルされた映像および／または音のデータ、および、前記対応関係情報生成手段からの対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを備えたことを特徴とする録画装置である。

【００２３】請求項２２の本発明は、請求項２０または２１記載の所定の記録媒体からの、請求項２０または２１記載の対応関係情報を入力し、その対応関係情報に基づいて、再生しようとするスクランブルされた映像および／または音のデータに対応するスクランブル鍵を特定し、さらに、そのスクランブル鍵が所定の条件に合うかどうかを判定し、合致する場合は、そのスクランブル鍵を、請求項２０または２１記載の格納手段から取り出し、合致しない場合は、そのスクランブル鍵を前記格納手段から取り出さないスクランブル鍵取得手段と、前記所定の記録媒体からの、前記再生しようとするスクランブルされた映像および／または音のデータに対応する、スクランブルされた映像および／または音のデータを入力するとともに、前記スクランブル鍵取得手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記スクランブルされた映像および／または音のデータのスクランブルを解除するスクランブル解除手段とを備えたことを特徴とする再生装置である。

【００２４】

【発明の実施の形態】以下に、本発明の実施の形態を図面を参照して説明する。

【００２５】（実施の形態１）先ず、本発明の実施の形態１の録画装置および再生装置の構成を述べる。

【００２６】図１に、本発明の実施の形態１の録画装置および再生装置のブロック図を示す。本発明の実施の形態１の録画装置は、第１鍵発生手段６と、記録スクランブル手段７と、第２鍵発生手段８と、ＫｃＦＩＦＯ９と、鍵暗号化手段１０と、対応関係情報生成手段１１と、ＭＵＸ１２から構成される。また、本発明の実施の形態１の再生装置は、第２ＤＭＵＸ１３と、暗号化鍵取得手段１４と、Ｋｃラッチ手段１５と、鍵解読手段１６と、再生デスクランブル手段１７から構成される。なお、図１には、受信復調手段１と、第１ＤＭＵＸ２と、ＥＭＭ解読手段３と、ＥＣＭ解読手段４と、放送デスクランブル手段５と、映像デコーダ１８と、音デコーダ１９も表示する。さらに、記録媒体としてのビデオテープ２０と、映像を表示し、音を出力するディスプレイ２１も表示する。

【００２７】受信復調手段１は、放送局からの、デジィタルの映像データ、音データ、ＥＭＭ（個別情報）、ＥＣＭ（番組情報）および暗号化された放送スクランブル鍵Ｋｓを通信衛星を介して入力し、それらの全部または一部の信号波形を整形する手段である。

【００２８】なお、受信復調手段１が入力する映像データおよび音データは、放送スクランブル鍵Ｋｓによりスクランブルされたデータである。また、以下では、映像データと音データの両方を意味する場合、映像データおよび音データをＡＶデータとする。

【００２９】また、受信復調手段１が入力するＥＭＭ（個別情報）は、後に説明するワーク鍵Ｋｗという鍵を生成するさいに必要となる情報である。

【００３０】さらに、受信復調手段１が入力するＥＣＭ（番組情報）は、暗号化された放送スクランブル鍵Ｋｓを復元するさいに必要となる情報である。

【００３１】さて、第１ＤＭＵＸ２は、受信復調手段１からの、波形整形された映像データ、音データ、ＥＭＭ、ＥＣＭおよび暗号化された放送スクランブル鍵Ｋｓを分離する手段であるとともに、放送デスクランブル手段５からの、デスクランブルされた映像データおよび音データを分離する手段である。また、第１ＤＭＵＸ２は、再生デスクランブル手段１７からの映像データおよび音データを分離する手段でもある。

【００３２】ＥＭＭ解読手段３は、ユーザＩＤ鍵Ｋｍを入力するとともに、第１ＤＭＵＸ２からのＥＭＭを入力し、ユーザＩＤ鍵ＫｍでＥＭＭを解読してワーク鍵Ｋｗを生成する手段である。

【００３３】ＥＣＭ解読手段４は、ＥＭＭ解読手段３からのワーク鍵Ｋｗを入力するとともに、第１ＤＭＵＸ２からのＥＣＭおよび暗号化された放送スクランブル鍵Ｋｓを入力し、ワーク鍵ＫｗでＥＣＭを解読して放送スクランブル鍵Ｋｓを復元する手段である。

【００３４】放送デスクランブル手段５は、ＥＣＭ解読手段４からの放送スクランブル鍵Ｋｓを入力するととも

に、第１ＤＭＵＸ２からの、スクランブルされたＡＶデータを入力し、放送スクランブル鍵Ｋｓで、スクランブルされたＡＶデータをデスクランブルする手段である。

【００３５】第１鍵発生手段６は、放送デスクランブル手段５によってデスクランブルされたＡＶデータを、再度スクランブルするための記録スクランブル鍵Ｋｓｓを発生する手段である。

【００３６】記録スクランブル手段７は、放送デスクランブル手段５からのＡＶデータを入力するとともに、第１鍵発生手段６からの記録スクランブル鍵Ｋｓｓを入力し、その記録スクランブル鍵ＫｓｓでＡＶデータをスクランブルする手段である。なお、以下では、記録スクランブル鍵ＫｓｓによりスクランブルされたＡＶデータをＫｓｓ（ＡＶデータ）とする。

【００３７】第２鍵発生手段８は、第１鍵発生手段６が発生した記録スクランブル鍵Ｋｓｓを暗号化するための暗号化鍵Ｋｃを発生する手段である。なお、第２鍵発生手段８は、毎日異なる暗号化鍵Ｋｃを発生するものとし、それら異なるＫｃをそれぞれＫｃ１、Ｋｃ２、Ｋｃ３、…とする。また、暗号化鍵Ｋｃ１、Ｋｃ２、Ｋｃ３、…それぞれは、１週間で廃棄されるものであるとする。

【００３８】ＫｃＦＩＦＯ９は、第２鍵発生手段８からの暗号化鍵Ｋｃ１、Ｋｃ２、Ｋｃ３、…を入力し格納する手段であるとともに、タイマーを有していて、そのタイマーを利用して、入力後１週間経過した暗号化鍵Ｋｃを廃棄する、ファーストインファーストアウト機能を有する手段である。

【００３９】鍵暗号化手段１０は、第１鍵発生手段６からの記録スクランブル鍵Ｋｓｓを入力するとともに、ＫｃＦＩＦＯ９からの暗号化鍵Ｋｃを入力し、その暗号化鍵Ｋｃで記録スクランブル鍵Ｋｓｓを暗号化する手段である。なお、以下では、暗号化鍵Ｋｃにより暗号化された記録スクランブル鍵ＫｓｓをＫｃ（Ｋｓｓ）とする。

【００４０】対応関係情報生成手段１１は、記録スクランブル鍵ＫｓｓによりスクランブルされたＡＶデータと、その記録スクランブル鍵Ｋｓｓを暗号化した暗号化鍵Ｋｃとを対応付けるための情報として、暗号化鍵Ｋｃ４が発生された日時の情報を生成する手段である。

【００４１】ＭＵＸ１２は、記録スクランブル手段７からのＫｓｓ（ＡＶデータ）と、鍵暗号化手段１０からのＫｃ（Ｋｓｓ）と、対応関係情報生成手段１１からの日時情報とを入力し、それらをビデオテープ２０に記録する手段である。

【００４２】第２ＤＭＵＸ１３は、ビデオテープ２０に記録された、Ｋｓｓ（ＡＶデータ）、Ｋｃ（Ｋｓｓ）および日時情報を入力し、それらを分離する手段である。

【００４３】暗号化鍵取得手段１４は、第２ＤＭＵＸ１３からの日時情報を入力し、その日時情報に基づいて、再生しようとするＫｓｓ（ＡＶデータ）に対応する暗号化鍵Ｋｃを特定し、その特定した暗号化鍵ＫｃをＫｃＦＩＦＯ９のなかから取得する手段である。

【００４４】Ｋｃラッチ手段１５は、暗号化鍵取得手段１４からの暗号化鍵Ｋｃを入力してラッチし、鍵解読手段１６に出力する手段である。

【００４５】鍵解読手段１６は、第２ＤＭＵＸ１３からのＫｃ（Ｋｓｓ）を入力するとともに、Ｋｃラッチ手段１５からの暗号化鍵Ｋｃを入力し、その暗号化鍵ＫｃでＫｃ（Ｋｓｓ）を解読し、記録スクランブル鍵Ｋｓｓを復元する手段である。

【００４６】再生デスクランブル手段１７は、第２ＤＭＵＸ１３からのＫｓｓ（ＡＶデータ）を入力するとともに、鍵解読手段１６からの記録スクランブル鍵Ｋｓｓを入力し、その記録スクランブル鍵ＫｓｓでＫｓｓ（ＡＶデータ）をデスクランブルする手段である。

【００４７】映像デコーダ１８は、第１ＤＭＵＸ２からの映像データを復号する手段である。

【００４８】音デコーダ１９は、第１ＤＭＵＸ２からの音データを復号する手段である。

【００４９】なお、請求項１の本発明の、スクランブル手段として記録スクランブル手段７、暗号化鍵発生手段として第２鍵発生手段８、格納手段としてＫｃＦＩＦＯ９、鍵暗号化手段として鍵暗号化手段１０、対応関係情報生成手段として対応関係情報生成手段１１、記録手段としてＭＵＸ１２を用いた。また、請求項６の本発明のスクランブル鍵発生手段として第１鍵発生手段６を、本実施の形態では用いた。さらに、請求項７の本発明の、暗号化鍵取得手段として暗号化鍵取得手段１４、鍵暗号化解読手段として鍵解読手段１６、スクランブル解除手段として再生デスクランブル手段１７を用いた。

【００５０】次に、このような本発明の実施の形態１の録画装置の動作を述べる。

【００５１】先ず、受信復調手段１は、放送局からの、デジィタルの映像データ、音データ、ＥＭＭ（個別情報）、ＥＣＭ（番組情報）および暗号化された放送スクランブル鍵Ｋｓを入力し、映像データおよび音データの信号波形の乱れを整形し、映像データ、音データ、ＥＭＭ、ＥＣＭおよび暗号化された放送スクランブル鍵Ｋｓを第１ＤＭＵＸ２に出力する。

【００５２】その後、第１ＤＭＵＸ２は、受信復調手段１からの映像データ、音データ、ＥＭＭ、ＥＣＭおよび放送スクランブル鍵Ｋｓを入力して分離し、映像データおよび音データ（ＡＶデータ）を放送デスクランブル手段５に出力する。また、ＥＭＭをＥＭＭ解読手段３に出力し、ＥＣＭおよび暗号化された放送スクランブル鍵ＫｓをＥＣＭ解読手段４に出力する。

【００５３】次に、ＥＭＭ解読手段３は、ユーザＩＤ鍵Ｋｍを入力するとともに、第１ＤＭＵＸ２からのＥＭＭを入力し、ユーザＩＤ鍵ＫｍでＥＭＭを解読してワーク鍵Ｋｗを生成し、ＥＣＭ解読手段４に出力する。

【００５４】さらに、ＥＣＭ解読手段４は、ＥＭＭ解読手段３からのワーク鍵Ｋｗを入力するとともに、第１ＤＭＵＸ２からの、ＥＣＭおよび暗号化された放送スクランブル鍵Ｋｓを入力し、ワーク鍵ＫｗでＥＣＭを解読して、暗号化された放送スクランブル鍵Ｋｓの暗号化を復元し、放送デスクランブル手段５に出力する。そして、放送デスクランブル手段５は、ＥＣＭ解読手段４からの放送スクランブル鍵Ｋｓを入力するとともに、第１ＤＭＵＸ２からの、スクランブルされたＡＶデータを入力し、放送スクランブル鍵Ｋｓで、スクランブルされたＡＶデータをデスクランブルする。そして、放送デスクランブル手段５は、デスクランブルされたＡＶデータを第１ＤＭＵＸ２または記録スクランブル手段７に出力する。なお、放送デスクランブル手段５は、リアルタイムでＡＶデータを直接ディスプレイ２１に表示させる場合に第１ＤＭＵＸ２に出力し、ビデオテープ２０にＡＶデータを記録させる場合に記録スクランブル手段７に出力する。ただし、ビデオテープ２０に記録されるＡＶデータは、放送デスクランブル手段５からの、そのままのＡＶデータではなく、再度スクランブルされたデータである。

【００５５】はじめに、放送デスクランブル手段５がＡＶデータを第１ＤＭＵＸ２に出力する場合について説明する。

【００５６】その場合、第１ＤＭＵＸ２は、放送デスクランブル手段５からのＡＶデータ入力し、それを映像データと音データに分離して、映像データを映像デコーダ１８に出力し、音データを音デコーダ１９に出力する。その後、映像デコーダ１８および音デコーダ１９それぞれは、第１ＤＭＵＸ２からの映像データまたは音データを復号し、ディスプレイ２１に出力する。そして、ディスプレイ２１は、映像を表示し音を出力する。

【００５７】次に、放送デスクランブル手段５がＡＶデータを記録スクランブル手段７に出力する場合について説明する。つまり、上述したように、ビデオテープ２０にＡＶデータを記録する場合である。

【００５８】先ず、記録スクランブル手段７は、放送デスクランブル手段５からの、デスクランブルされたＡＶデータを入力する。

【００５９】そして、第１鍵発生手段６は、記録スクランブル手段７が入力したＡＶデータをスクランブルするための記録スクランブル鍵Ｋｓｓを発生し、記録スクランブル手段７および鍵暗号化手段１０に出力する。

【００６０】次に、記録スクランブル手段７は、第１鍵発生手段６からの記録スクランブル鍵Ｋｓｓを入力し、その記録スクランブル鍵ＫｓｓでＡＶデータをスクランブルする。つまり、Ｋｓｓ（ＡＶデータ）を生成する。そして、Ｋｓｓ（ＡＶデータ）を対応関係情報生成手段１１およびＭＵＸ１２に出力する。

【００６１】他方、第２鍵発生手段８は、第１鍵発生手段６が発生した記録スクランブル鍵Ｋｓｓを暗号化するための暗号化鍵Ｋｃを発生する。その第２鍵発生手段８が発生する暗号化鍵Ｋｃは毎日異なるものとする。ここでは、以下の説明の便宜上、録画装置が動作し始める日を１９９８年１月１日であるとし、記録時である本日をその日から３日後の１９９８年１月４日であるとし、図２の暗号化鍵Ｋｃリスト（ａ）に示すように、１月１日に発生された暗号化鍵ＫｃをＫｃ１、１月２日に発生された暗号化鍵ＫｃをＫｃ２、…、１月４日に発生された暗号化鍵ＫｃをＫｃ４とする。また、以下、同様にして暗号化鍵Ｋｃは発生されるものとする。なお、ことわりがない限り、以下、１月４日の録画装置の動作について説明する。

【００６２】さて、ＫｃＦＩＦＯ９は、図２（ａ）のリストに示すように、１月１日から毎日一つづつの暗号化鍵Ｋｃを第２鍵発生手段８から既に入力して格納し、１月３日までに暗号化鍵Ｋｃ１、Ｋｃ２、Ｋｃ３を格納しておき、本日１月４日には、Ｋｃ４を入力して格納する。その格納は、常に最新の暗号化鍵Ｋｃが図２（ａ）のリストのトップの順位にくるように行われ、また、古いものは順次順位を下げるように行われる。なお、ＫｃＦＩＦＯ９は、格納した暗号化鍵Ｋｃ１、Ｋｃ２、…を、それぞれの格納から１週間経過した後に廃棄する。例えば、図２（ｂ）のリストに示すように、１月９日になると、Ｋｃ１、Ｋｃ２という暗号化鍵は廃棄され、ＫｃＦＩＦＯ９は、Ｋｃ９、Ｋｃ８、…、Ｋｃ４、Ｋｃ３という順序で７つの暗号化鍵を格納することになる。つまり、ＫｃＦＩＦＯ９が格納する暗号化鍵Ｋｃの数は７までである。

【００６３】次に、鍵暗号化手段１０は、第１鍵発生手段６からの記録スクランブル鍵Ｋｓｓを入力するとともに、ＫｃＦＩＦＯ９を介して、第２鍵発生手段８が記録時である１月４日に発生した暗号化鍵Ｋｃ４を入力し、その暗号化鍵Ｋｃ４で記録スクランブル鍵Ｋｓｓを暗号化する。つまり、Ｋｃ４（Ｋｓｓ）を生成する。

【００６４】そして、対応関係情報生成手段１１は、記録スクランブル手段７からのＫｓｓ（ＡＶデータ）と、鍵暗号化手段１０からのＫｃ４（Ｋｓｓ）とを入力し、その暗号化鍵Ｋｃ４と、その暗号化鍵Ｋｃ４で暗号化された記録スクランブル鍵ＫｓｓによりスクランブルされたＡＶデータとを対応付けるための情報として、その暗号化鍵Ｋｃ４が発生された日時の情報を生成する。つまり、１月４日という日時情報を生成する。

【００６５】その後、ＭＵＸ１２は、記録スクランブル手段７からのＫｓｓ（ＡＶデータ）と、鍵暗号化手段１０からのＫｃ４（Ｋｓｓ）と、対応関係情報生成手段１１からの１月４日という日時情報とを入力し、それらを１組としてビデオテープ２０に記録する。

【００６６】このようにして、毎日、その日に発生された暗号化鍵Ｋｃｎ（ｎ＝１、２、…）に対応するＫｃｎ

（Ｋｓｓ）と、Ｋｓｓ（ＡＶデータ）と、その日の日時情報とが１組となってビデオテープ２０に記録される。

【００６７】次に、本発明の実施の形態１の再生装置の動作を述べる。

【００６８】つまり、録画装置によってビデオテープ２０に記録されたＫｓｓ（ＡＶデータ）を再生する場合について説明する。

【００６９】以下の説明の便宜上、再生装置がビデオテープ２０のＫｓｓ（ＡＶデータ）を再生する日を１月９日であるとする。そして、再生装置は、１月１日にビデオテープ２０に記録されたＫｓｓ（ＡＶデータ）と、１月３日にビデオテープ２０に記録されたＫｓｓ（ＡＶデータ）とを再生しようとするものとする。

【００７０】はじめに、再生装置が１月１日にビデオテープ２０に記録されたＫｓｓ（ＡＶデータ）を再生しようとする場合について説明する。

【００７１】先ず、第２ＤＭＵＸ１３は、ビデオテープ２０からの、１月１日に記録されたＫｓｓ（ＡＶデータ）と、Ｋｃ１（Ｋｓｓ）と、１月１日という日時情報とを入力し、それらを分離し、１月１日という日時情報を暗号化鍵取得手段１４に出力する。

【００７２】そして、暗号化鍵取得手段１４は、その１月１日という日時情報を入力し、その日時情報に基づいて、暗号化鍵Ｋｃ１を特定し、ＫｃＦＩＦＯ９が格納している、図２（ｂ）のリストのなかから暗号化鍵Ｋｃ１を検索する。しかしながら、その暗号化鍵Ｋｃ１は、発生から一週間以上経過しているので、ＫｃＦＩＦＯ９により廃棄されており、図２（ｂ）のリストのなかには存在しない。したがって、暗号化鍵取得手段１４は、暗号化鍵Ｋｃ１を取得することができない。その結果、再生デスクランブル手段１７は、その暗号化鍵Ｋｃ１を間接的に用いてデスクランブルする必要がある、１月１日に記録されたＫｓｓ（ＡＶデータ）をデスクランブルすることができなくなり、そのＡＶデータがディスプレイ２１に出力されても、解読不能なため、ディスプレイ２１は、ＡＶデータ本来の映像および音を出力することができない。

【００７３】次に、再生装置が１月３日にビデオテープ２０に記録されたＫｓｓ（ＡＶデータ）を再生しようとする場合について説明する。

【００７４】先ず、第２ＤＭＵＸ１３は、ビデオテープ２０からの、１月３日に記録されたＫｓｓ（ＡＶデータ）と、Ｋｃ３（Ｋｓｓ）と、１月３日という日時情報とを入力し、それらを分離し、１月３日という日時情報を暗号化鍵取得手段１４に出力する。

【００７５】次に、暗号化鍵取得手段１４は、その１月３日という日時情報を入力し、その日時情報に基づいて、暗号化鍵Ｋｃ３を特定し、ＫｃＦＩＦＯ９が格納している、図２（ｂ）のリストのなかから暗号化鍵Ｋｃ３を検索してその暗号化鍵Ｋｃ３を取得し、それをＫｃラッチ手段１５に出力する。

【００７６】その後、Ｋｃラッチ手段１５は、暗号化鍵Ｋｃ３を入力し、鍵解読手段１６に出力する。また、第２ＤＭＵＸ１３は、Ｋｃ３（Ｋｓｓ）を鍵解読手段１６に出力する。

【００７７】そして、鍵解読手段１６は、第２ＤＭＵＸ１３からのＫｃ３（Ｋｓｓ）を入力するとともに、Ｋｃラッチ手段１５からの暗号化鍵Ｋｃ３を入力し、その暗号化鍵Ｋｃ３でＫｃ３（Ｋｓｓ）を解読し、記録スクランブル鍵Ｋｓｓを復元して、その記録スクランブル鍵Ｋｓｓを再生デスクランブル手段１７に出力する。また、第２ＤＭＵＸ１３は、Ｋｓｓ（ＡＶデータ）を鍵解読手段１６に出力する。

【００７８】次に、再生デスクランブル手段１７は、第２ＤＭＵＸ１３からのＫｓｓ（ＡＶデータ）を入力するとともに、鍵解読手段１６からの記録スクランブル鍵Ｋｓｓを入力し、その記録スクランブル鍵ＫｓｓでＫｓｓ（ＡＶデータ）をデスクランブルして、そのデスクランブルされたＡＶデータを第１ＤＭＵＸ２に出力する。

【００７９】そして、第１ＤＭＵＸ２は、再生デスクランブル手段１７からのＡＶデータを入力し、それを映像データと音データに分離して、映像データを映像デコーダ１８に出力し、音データを音デコーダ１９に出力する。その後、映像デコーダ１８および音デコーダ１９それぞれは、第１ＤＭＵＸ２からの映像データまたは音データを復号し、ディスプレイ２１に出力する。そして、ディスプレイ２１は、映像を表示し音を出力する。

【００８０】このようにして、ビデオテープ２０に記録されたＫｓｓ（ＡＶデータ）それぞれは、記録されてから１週間以内でないと、最終的に、本来の映像および音声として再生されない。

【００８１】なお、上述した実施の形態１では、ビデオテープ２０に記録されたＫｓｓ（ＡＶデータ）それぞれは、記録されてから１週間以内であれば再生されるとしたが、１週間以内というような期間の制限ではなく、Ｋｓｓ（ＡＶデータ）それぞれの再生回数を、例えば１回や３回というように制限して、その制限再生回数内でないと、再生されないとしてもよい。つまり、図３に示すように、本発明の再生装置がカウンタ２２を備え、そのカウンタ２２が各Ｋｓｓ（ＡＶデータ）の再生回数をチェックし、例えば１回や３回というような制限された再生回数に達した場合、ＫｃＦＩＦＯ９が、そのＫｓｓ（ＡＶデータ）に対応する暗号化鍵Ｋｃを廃棄するとしてもよい。また、上述した１週間以内というような期間の制限と再生回数の制限を併用するとしてもよい。

【００８２】また、上述した実施の形態１では、ＫｃＦＩＦＯ９は、格納した暗号化鍵Ｋｃを１週間経過した後に廃棄するとした。しかし、ＫｃＦＩＦＯ９は、格納した暗号化鍵Ｋｃを１週間経過しても廃棄せずに、格納したままにしておき、暗号化鍵取得手段１４が、Ｋｓｓ

（ＡＶデータ）を再生しようとする日が暗号化鍵Ｋｃの発生から１週間以内か否かを判断して、または、制限回数内か否かを判断して、１週間以内または制限回数内以内であれば、再生しようとするＫｓｓ（ＡＶデータ）に対応する暗号化鍵ＫｃをＫｃＦＩＦＯ９から取得できるとしてもよい。したがって、この場合、請求項８の本発明では、スクランブル手段として記録スクランブル手段７、暗号化鍵発生手段として第２鍵発生手段８、格納手段としてＫｃＦＩＦＯ９、鍵暗号化手段として鍵暗号化手段１０、対応関係情報生成手段として対応関係情報生成手段１１、記録手段としてＭＵＸ１２がそれぞれ該当することになる。また、請求項１２の本発明では、暗号化鍵取得手段として暗号化鍵取得手段１４、鍵暗号化解読手段として鍵解読手段１６、スクランブル解除手段として再生デスクランブル手段１７がそれぞれ該当することになる。

【００８３】また、上述した実施の形態１では、第１鍵発生手段６は、記録スクランブル手段７が入力したＡＶデータをスクランブルするための記録スクランブル鍵Ｋｓｓを発生するとした。しかし、本発明の録画装置は、図４に示すように、第１鍵発生手段６を備えず、記録スクランブル手段７は、放送局から送られてくる放送スクランブル鍵Ｋｓを、放送デスクランブル手段５を介して入力し、その放送スクランブル鍵Ｋｓで、または、その放送スクランブル鍵Ｋｓを加工したもので、ＡＶデータをスクランブルするとしてもよい。その場合、鍵暗号化手段１０は、記録スクランブル手段７から、放送スクランブル鍵Ｋｓ、または、その放送スクランブル鍵Ｋｓを加工したものを入力し、それを暗号化鍵Ｋｃで暗号化する。

【００８４】また、上述した実施の形態１では、記録スクランブル手段７は、第１鍵発生手段６からの記録スクランブル鍵ＫｓｓでＡＶデータをスクランブルするとした。しかし、本発明の録画装置は、図５に示すように、第１鍵発生手段６、鍵暗号化手段１０を備えず、記録スクランブル手段７は、第２鍵発生手段８からの暗号化鍵ＫｃをＫｃＦＩＦＯ９を介して入力し、その暗号化鍵Ｋｃを記録スクランブル鍵Ｋｃとして使用し、その記録スクランブル鍵Ｋｃにより、ＡＶデータをスクランブルするとしてもよい。この場合、ビデオテープ２０には、記録スクランブル鍵Ｋｃによりスクランブルされ
たＡＶデータ、つまり、Ｋｃ（ＡＶデータ）と、記録スクランブル鍵Ｋｃとが記録される。またその場合、本発明の再生装置は、図５に示すように、鍵解読手段１６を備えないことになる。したがって、Ｋｃ（ＡＶデータ）を再生しようとする場合、スクランブル鍵取得手段２３は、対応する記録スクランブル鍵Ｋｃを特定し、それをＫｃＦＩＦＯ９のなかから取得する。そして、再生デスクランブル手段１７は、ビデオテープ２０からのＫｃ（ＡＶデータ）を第２ＤＭＵＸ１３を介して入力するとともに、スクランブル鍵取得手段２３からの記録スクランブル鍵ＫｃをＫｃラッチ手段１５を介して入力し、その記録スクランブル鍵ＫｃでＫｃ（ＡＶデータ）をデスクランブルする。そのため、この場合、つまり、請求項１５および２０の本発明では、スクランブル鍵発生手段として第２鍵発生手段８、格納手段としてＫｃＦＩＦＯ９、スクランブル手段として記録スクランブル手段７、対応関係情報生成手段として対応関係情報生成手段１１、記録手段として第１ＤＭＵＸ２がそれぞれ該当することになる。また、請求項１９および２２の本発明では、スクランブル鍵取得手段としてスクランブル鍵取得手段２３、スクランブル解除手段として再生デスクランブル手段１７がそれぞれ該当することになる。

【００８５】また、上述した実施の形態１の録画装置は、図６に示すように、課金手段２４を備え、ビデオテープ２０にＫｓｓ（ＡＶデータ）を記録するさい、その記録に対する所定の課金をユーザに課し、あらかじめユーザから所定の料金が放送局等に支払われた場合、もしくは、少なくとも記録するさいに所定の料金が支払われた場合のみ、Ｋｓｓ（ＡＶデータ）はビデオテープ２０に記録されるとしてもよい。また、課金手段２４は、図６に示す位置に配置されなくとも、鍵暗号化手段１０とＭＵＸ１２との間に配置されるとしてもよい。要するに、課金手段２４は、ビデオテープ２０にＫｓｓ（ＡＶデータ）を記録するさい、その記録に対する所定の課金をユーザに課すものでありさえすればよく、配置場所はどの場所であってもよい。

【００８６】また、上述した実施の形態１では、暗号化鍵Ｋｃそれぞれは、発生から１週間経過すると廃棄されるとしたが、廃棄される日時は、発生から１週間経過後に限定することはなく、１日経過後であっても、３日経過後であっても、または、１２時間経過後であってもよい。要するに、暗号化鍵Ｋｃそれぞれは、発生から所定の期間経過すると廃棄されさえすればよい。

【００８７】また、上述した実施の形態１では、第２鍵発生手段８は、毎日、１つづつ異なる暗号化鍵Ｋｃを発生するとしたが、第２鍵発生手段８は、同じ日であっても、数時間毎に異なる暗号化鍵Ｋｃを発生するとしてもよい。さらに、ビデオテープ２０に所定の番組のＫｓｓ（ＡＶデータ）を記録する毎に暗号化鍵Ｋｃを発生するとしてもよい。つまり、一回の録画開始からその録画の終了毎に、その都度、暗号化鍵Ｋｃを発生するとしてもよい。要するに、第２鍵発生手段８は、記録しようとするＫｓｓ（ＡＶデータ）の記録スクランブル鍵Ｋｓｓを暗号化するための暗号化鍵Ｋｃを発生しさえすればよい。

【００８８】また、上述した実施の形態１では、本発明の対応関係情報として、暗号化鍵Ｋｃが発生されたさいの日時情報を用いたが、本発明の対応関係情報は、記録スクランブル手段７がＡＶデータを入力した日時、記録

スクランブル手段７が記録スクランブル鍵ＫｓｓでＡＶデータをスクランブルした日時、第２鍵発生手段８が暗号化鍵Ｋｃを発生した日時、ＫｃＦＩＦＯ９が暗号化鍵Ｋｃを格納した日時、鍵暗号化手段１０が暗号化鍵Ｋｃで記録スクランブル鍵Ｋｓｓを暗号化した日時、または、ＭＵＸ１２がビデオテープ２０にＫｓｓ（ＡＶデータ）を記録した日時の情報であってもよい。もしくは、上述した暗号化鍵Ｋｃが発生されたさいの日時や、記録スクランブル手段７がＡＶデータを入力した日時等と、ＡＶデータを再生しようとする日時との情報であってもよい。その場合、図２の暗号化鍵Ｋｃリストの各暗号化鍵Ｋｃが毎日順位を下げることに基づいて、また、２つの日時の差が考慮されて、暗号化鍵Ｋｃが取得されることになる。または、本発明の対応関係情報は、上述した暗号化鍵Ｋｃが発生されたさいの日時や、記録スクランブル手段７がＡＶデータを入力した日時等と、ＡＶデータを再生しようとする日時とに基づき、また、図２の暗号化鍵Ｋｃリストの各暗号化鍵Ｋｃが毎日順位を下げることが考慮された、図２の暗号化鍵Ｋｃリストの番号情報等であってもよい。

【００８９】また、上述した実施の形態１では、記録媒体としてのビデオテープ２０を用いたが、記録媒体は、ビデオテープ２０に限らず、ハードディスクであってもよい。

【００９０】また、上述した実施の形態１では、第１鍵発生手段６はＡＶデータをスクランブルするための記録スクランブル鍵Ｋｓｓを発生するが、その記録スクランブル鍵Ｋｓｓは、簡単に解読することができないように、例えば数十秒などの短い期間で更新されるとしてもよい。

【００９１】さらに、上述した録画装置または再生装置は、暗号化鍵Ｋｃの発生から例えば１週間という所定の期間を経過するなどして、その暗号化鍵Ｋｃが廃棄されたり、使用不可になる前に、その暗号化鍵Ｋｃに対応するＫｓｓ（ＡＶデータ）が一度も再生されていない場合、その旨の情報をユーザに通知する手段を備えてもよい。

【００９２】

【発明の効果】以上説明したところから明らかなように、本発明は、ＡＶデータを記録媒体に記録し、そのＡＶデータの有効再生期間や有効再生回数の制限を遵守する録画装置および再生装置を提供することができる。

【図面の簡単な説明】

【図１】本発明の実施の形態１の録画装置および再生装置のブロック図

【図２】本発明の実施の形態１の録画装置および再生装置に使用される暗号化鍵Ｋｃリストの一例を示す図

【図３】図１とは異なる本発明の録画装置および再生装置のブロック図

【図４】図１または３とは異なる本発明の録画装置および再生装置のブロック図

【図５】図１、３または４とは異なる本発明の録画装置および再生装置のブロック図

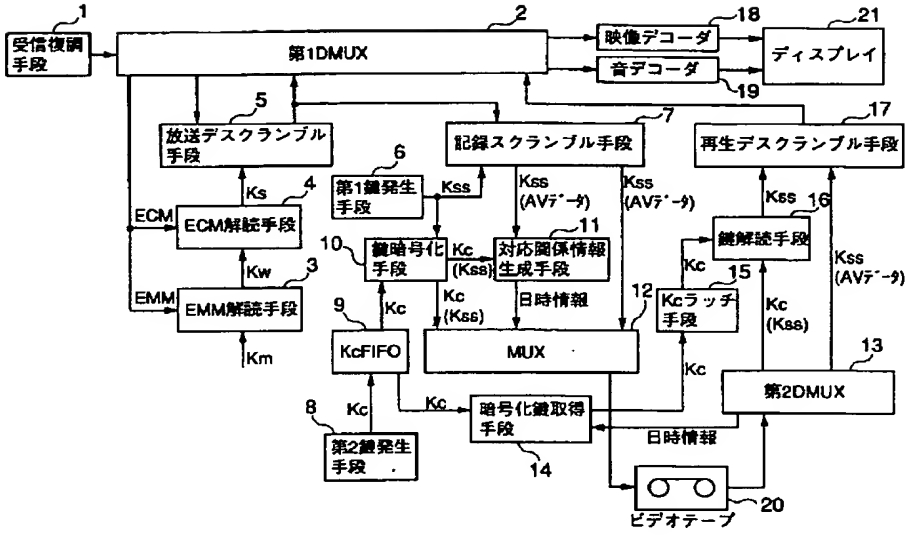
【図６】図１、３、４または５とは異なる本発明の録画装置および再生装置のブロック図

【図７】従来の録画再生装置のブロック図

【符号の説明】

１　受信復調手段
２　第１ＤＭＵＸ
３　ＥＭＭ解読手段
４　ＥＣＭ解読手段
５　放送デスクランブル手段
６　第１鍵発生手段
７　記録スクランブル手段
８　第２鍵発生手段
９　ＫｃＦＩＦＯ
１０　鍵暗号化手段
１１　対応関係情報生成手段
１２　ＭＵＸ
１３　第２ＤＭＵＸ
１４　暗号化鍵取得手段
１５　Ｋｃラッチ手段
１６　鍵解読手段
１７　再生デスクランブル手段
１８　映像デコーダ
１９　音デコーダ
２０　ビデオテープ
２１　ディスプレイ
２２　カウンタ
２３　スクランブル鍵取得手段
２４　課金手段

【図１】



【図２】

暗号化鍵 Kc リスト

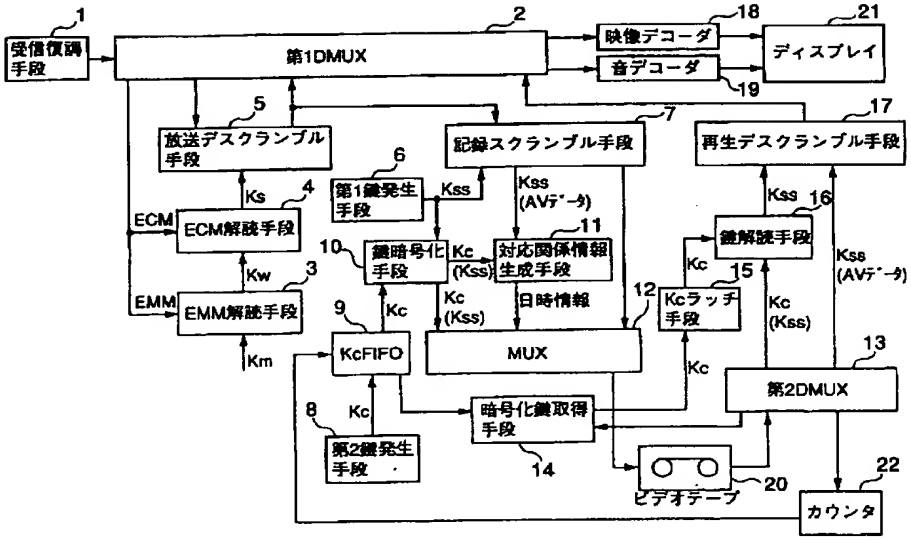
(a) 1月 4日 現在

No.	暗号化鍵	鍵発生日
1	Kc 4	1月 4日
2	Kc 3	1月 3日
3	Kc 2	1月 2日
4	Kc 1	1月 1日
5		
6		
7		

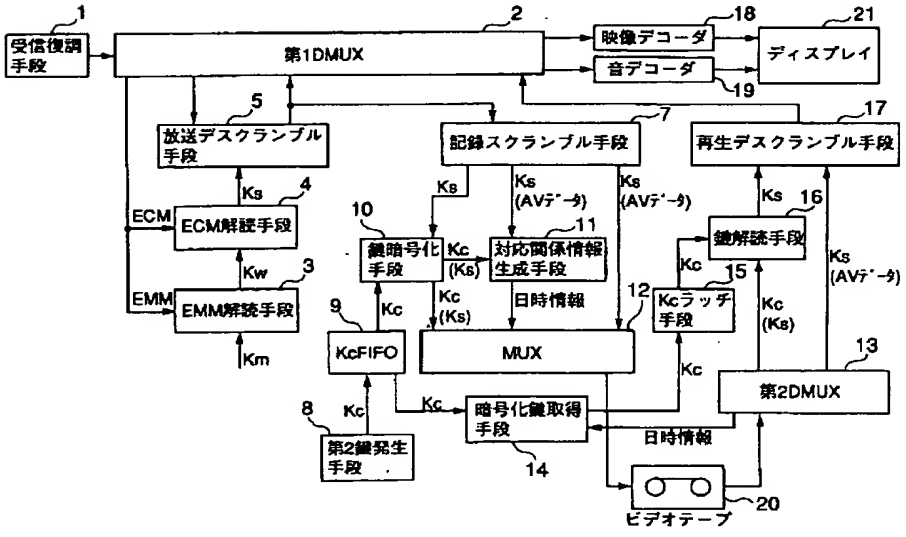
(b) 1月 9日 現在

No.	暗号化鍵	鍵発生日
1	Kc 9	1月 9日
2	Kc 8	1月 8日
3	Kc 7	1月 7日
4	Kc 6	1月 6日
5	Kc 5	1月 5日
6	Kc 4	1月 4日
7	Kc 3	1月 3日

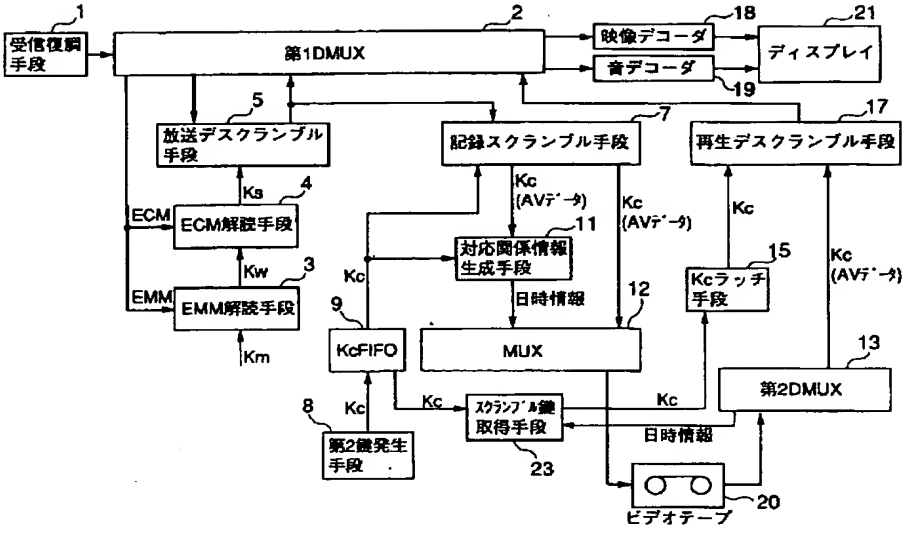
【図３】


受信復調手段
第1DMUX
映像デコーダ
音デコーダ
ディスプレイ
放送デスクランブル手段
記録スクランブル手段
再生デスクランブル手段
第1鍵発生手段
ECM
ECM解読手段
鍵暗号化手段
対応関係情報生成手段
鍵解読手段
EMM
EMM解読手段
Kcラッチ手段
KcFIFO
MUX
第2DMUX
暗号化鍵取得手段
第2鍵発生手段
ビデオテープ
カウンタ
Ks
Kss
Kss (AVデータ)
Kw
Km
Kc
Kc (Kss)
日時情報
Kss (AVデータ)

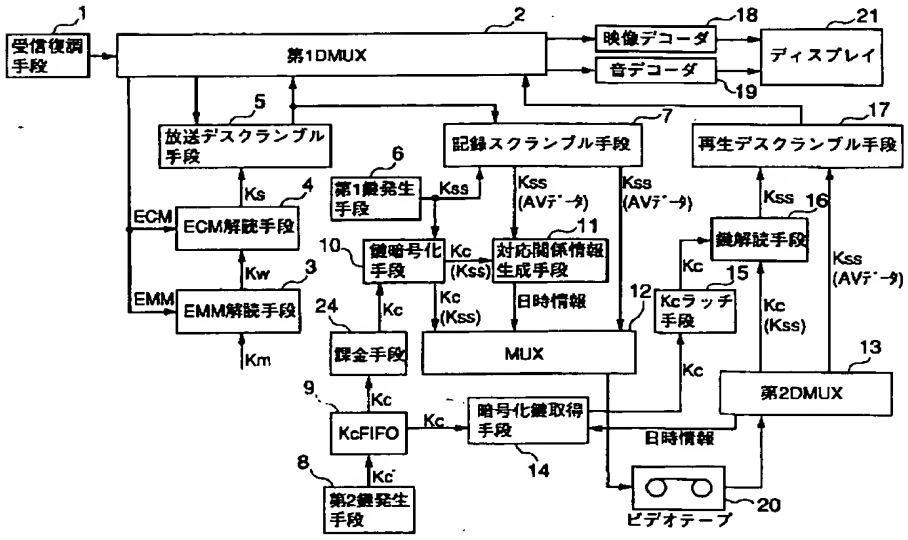
【図４】


受信復調手段
第1DMUX
映像デコーダ
音デコーダ
ディスプレイ
放送デスクランブル手段
記録スクランブル手段
再生デスクランブル手段
ECM
ECM解読手段
鍵暗号化手段
対応関係情報生成手段
鍵解読手段
EMM
EMM解読手段
Kcラッチ手段
KcFIFO
MUX
第2DMUX
暗号化鍵取得手段
第2鍵発生手段
ビデオテープ
Ks
Ks (AVデータ)
Kw
Km
Kc
Kc (Ks)
日時情報

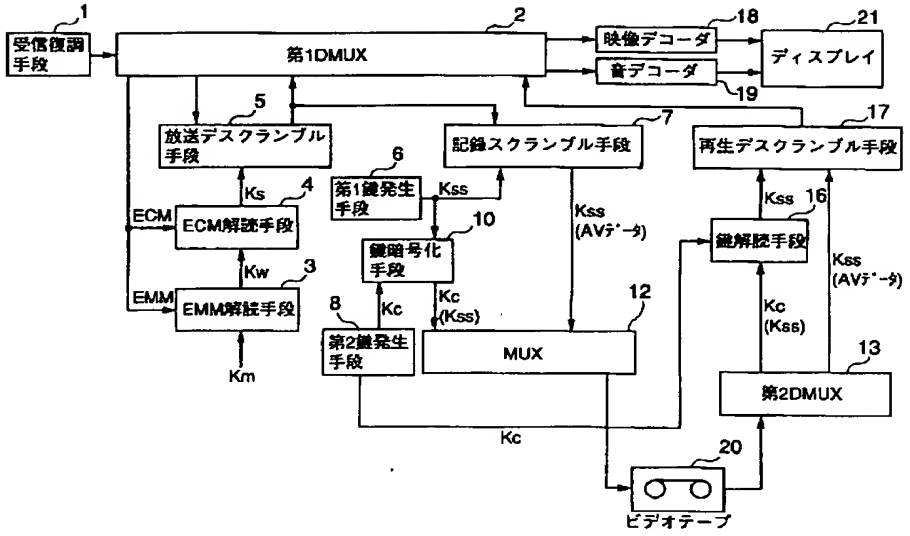
【図５】


受信復調手段
第1DMUX
映像デコーダ
音デコーダ
ディスプレイ
放送デスクランブル手段
記録スクランブル手段
再生デスクランブル手段
ECM
ECM解読手段
EMM
EMM解読手段
Ks
Kw
Km
Kc
(AVデータ)
対応関係情報生成手段
日時情報
KcFIFO
MUX
Kcラッチ手段
第2DMUX
第2鍵発生手段
スクランブル鍵取得手段
ビデオテープ

【図６】


受信復調手段
第1DMUX
映像デコーダ
音デコーダ
ディスプレイ
放送デスクランブル手段
記録スクランブル手段
再生デスクランブル手段
第1鍵発生手段
ECM
ECM解読手段
EMM
EMM解読手段
Ks
Kw
Km
Kss
(AVデータ)
鍵暗号化手段
対応関係情報生成手段
鍵解読手段
Kc
(Kss)
日時情報
課金手段
MUX
Kcラッチ手段
第2DMUX
KcFIFO
暗号化鍵取得手段
第2鍵発生手段
ビデオテープ

【図７】



フロントページの続き

(51) Int. Cl. 6		識別記号	F I		
Ｈ０４Ｎ	5/92		Ｈ０４Ｎ	5/92	Ｚ
// Ｈ０４Ｎ	7/167			7/167	Ｚ

(72) 発明者　後藤　昌一
大阪府門真市大字門真1006番地　松下電器
産業株式会社内